وزارة التعليـــم العالـــي والبحث العلمـــي
جامعة الحاج لخضر - باتنـــة-
كلية الحقـــــوق والعلوم السياسية
قســـم الحقـــوق

آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري

مذكرة مقدمة لنيل شهـــادة الماجستيـــر في العلوم القانونية
تخصص: علوم جنائية

إعداد الطالب:
سعيداني نعيم

إشراف:
أ. د. زرارة صالحي الواسعة

لجنـــــة المناقشـــــة:

الاســـم واللقب	الدرجـة العلميـة	الجامعـــة الأصليـة	الصفـة
د.خير الدين شمامة	أستاذ محاضر أ	جامعة الحاج لخضر- باتنة-	رئيســا
أ.د. زرارة صالحي الواسعة	أستاذة التعليم العالي	جامعة الحاج لخضر- باتنة-	مشرفا ومقررا
د.علـي قصير	أستاذ محاضر أ	جامعة الحاج لخضر- باتنة-	عضـوا مناقشا
د. بن حملة سامي	أستاذ محاضر أ	جامعة قسنطينة	عضـوا مناقشا

السنـــــة الجامعيـــــة:
2012-2013

الإهـــــداء

إلى من أوصاني بهما ربي برا وإحسانا والدي **أمـــي وأبـــي**

إلى رفيقة دربي **زوجـــــتي العزيزة**

إلى ريحانتي قلبي بنتاي العزيزتين **لمـــيس وريـــــم**

أهدي هذا العمل المتواضـــع

شكـــر وتقـــدير

يشرفني أن أتقدم بأسمى آيات الشكر والعرفان
إلى أستاذتي الفاضلة الأستاذة الدكتورة **زرارة صالحي الواســـعة**
التي تولت مهمة الإشراف على هذا البحث، كما لا يفوتني أن أخلص
بالشكر إلى كل من ساعدني ولو بالكلمة الطيبة.

مقدمـــــــــــة

مــقــدمة:

إن التطور الهائل الذي شهده كل من مجال تقنية المعلومات ومجال الإتصالاتوالإندماج المذهل الذي حدث بينهما فيما بعد، كان المحور الأساسي الذي قامت عليه تقنية المعلومات، إذ أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول،فبات يطلق على هذا العصر عصر المعلومات، فمنذ وقت ليس ببعيد كان كم المعلومات المتولدة عن التفاعلات البشرية محدودًا إلى حد كبير و لم يشكل حجمها أي مشكلة أمام عمليات تجميعها وتخزينها وإعادة استرجاعها ، إلا أنه ومع تقدم البشرية وتزايد معارف الإنسان وعلومه بدأ كم المعلومات يتزايد ويتكاثر وصارت الطرق التقليدية لتجميع وتنظيم هذه المعلوماتعاجزة عن تلبية احتياجات المستفيدين منها بكفاءة وفعالية، وأصبح من الضروري اللجوء إلى استخدام أساليب علمية وتقنية متطورة لمواجهة هذه الطفرة ، فكان أن ظهرت الحاسبات الإلكترونية ، بالإضافة إلى ظهور مستحدثات تقنية كأقراص الفيديو الرقمية وأقراص الليزر ، ووسائط الإتصال**...** وذلك من أجل تسهيل التحكم في المعلومات ومعالجتها واسترجاعها، وهو مادعا بالكثير من رجال الإقتصادوالإجتماع إلى وصف الثورة المعلوماتية بالثورة الصناعية الثانية بالمقارنة مع الثورة الصناعية الأولى التي تحققت في القرنين التاسع عشر والعشرين، ففي حين كان هدف الثورة الأولى إحلال الآلة محل الجهد البدني للإنسان ، فإن هدف الثورة الثانية هو إحلال الآلة محل النشاط الذهني للإنسان**.**

وفي مرحلة لاحقة من مسار عصر تقنية المعلومات تم التوصل إلى فكرة الربط بين أجهزة الإعلام الآلي، ووسائل الإتصال، الأمر الذي أثمر على ظهور شبكات المعلومات، ولعل أهمها على الإطلاق شبكة الانترنت (شبكة الشبكات)**.**

ثم استتبع اتساع ونماء كل من تكنولوجيا الإتصالات والحاسبات من جهة، والبرمجية بما تضمنته من هندسة البرمجيات وصناعتها من جهة أخرى،والإندماج المذهل الذي حدث بينهما إلى الوصول إلى استحداث تقنية نظم المعالجة الآلية للمعطيات.

ومن دون شك تضاعفت أهمية هذه التقنية وازداد الإعتماد عليها في نقل وتبادل المعلومات بالصوت والصورة عبر أنحاء العالم، نظرا لما تتميز به من شمول وسعة محتواها وماتوفره من مال وجهد ووقت،وأصبحت بذلك نظم المعالجة الآلية للمعطيات بسبب التقنيات التي تقوم عليها والمتمثلة في الحواسيب والشبكات المعلوماتية أكثر انتشارا في كل القطاعات والمجالات (كالصناعة والتجارة ، النقل ، الصحة ، التعليم ، الدفاع والبحوث ....) وبدا من الصعب أن تقوم هذه القطاعات بأداء أعمالها دون الإعتماد بشكل أساسي على هذه التقنية الحديثة ، فقد أصبحت من لوازم الحياة المتطورة سواء على المستوى العام أم الخاص، حيث تعتمد المؤسسات الحكومية والخاصة على حد سواء في تسيير أعمالها بشكل أساسي على استخدام نظم المعالجة الآلية.

لكن وعلى الرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة ، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الإنعكاسات السلبية والخطيرة جراء سوء استخدام هذه التقنية، ذلك أن الآثار الإيجابية المشرقة لعصر تقنية المعلومات لا تنف الإنعكاسات السلبية التي أفرزتها هذه التقنية ، نتيجة إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات، الشيء الذي استتبعه ظهور أنماط جديدة من الإعتداءات على تلك المعلومات المخزنة في بيئة افتراضية، ليس هذا فحسب بل سهلت هذه التقنية ارتكاب بعض الجرائم التقليدية، فازدادت هذه المخاطر تفاقما في ظل البيئة الإفتراضية التي تمثلها شبكة المعلومات، مما أفرز نوعا جديدا من الجرائم، لم يكن معهودا من قبل عرفت بالجرائم المعلوماتية، أو جرائم تقنية المعلومات .

والخطورة التي تتميز بها هذه الجرائم المستحدثة هي أنها سهلة الإرتكاب نتيجة للإستخدام السلبي للتقنية المعلوماتية بما توفره من تسهيلات، وأن آثارها ليست محصورة في النطاق الإقليمي لدولة بعينها، فضلا على أن مرتكبيها يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الإلية للمعطيات والإلمام بالمهارات والمعارف التقنية، ليس هذا فحسب بل إنها تستهدف محلا من طبيعة خاصة ونعني بذلك المعلومات التي يحتوي عليها نظام المعالجة الآلية، والذي هو عبارة عن إشارات ونبضات إلكترونية تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الإتصال العالمية بصورة آلية، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة (أجهزة العدالة الجنائية بجميع مستوياتها وعلى اختلاف أدوارها)وبالذات فيما يخص إثبات هذه الجرائم وآلية مباشرة إجراءات الإستدلال والتحقيق عبر البيئة الإفتراضية لتعقب المجرمين وتقديمهم للعدالة .

فإذا كانت الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين متعودة على التعامل مع الجريمة بصورتها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثار مادية في مسرح الجريمة من بصمات أو آثار أقدام أو بقع دم أو محررات مزورة ..... ، فإن المشكلات الإجرائية التي ستواجه هذه الجهات عند تعاملها مع الجريمة المعلوماتية، تبدأ من طبيعة البيئة الإفتراضيةالتقنية التي ترتكب فيها، فهي لا تخلفأي آثار مادية محسوسة، كما أن هذه الجريمة تتم في الخفاء، فكثيرا ما يعمد المجرم المعلوماتي إلى إخفاء نشاطه الجرمي عن طريق تلاعبهبالبيانات والذي غالبا ما يتحقق في غفلة من المجني عليه، فضلا عن سهولة تدمير الدليل ومحوه من مسرح الجريمة مما يعقد أمر كشفها وتحديد مرتكبها.

وعلى ضوء ذلك فإن هذه الظاهرة الإجرامية التقنية أثارت العديد من المشكلات في نطاق قانون الإجراءات الجزائية الذي وضعت نصوصه لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي.

وهو الأمر الذي كان عاملا حاسما لتدخل المشرع بنصوص قانونية إجرائية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، ليمكن من خلالها استنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم ووسائل ارتكابها، مما أدى إلى ظهور نوع جديد من الأدلة يمكن الإعتماد عليه في إثبات هذه الجرائم من ذات الطبيعة التقنية التي تتميز بها البيئة محل الجريمة المعلوماتية.

وقد كان ذلك بأن قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون 22/06المؤرخ في 20ديسمبر 2006، بالإضافة إلى إصداره للقانون 04/09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ، ومن خلالهما أوجد المشرع طرقا إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية

أهمية الـــبحث:

ويعد موضوع البحث من الموضوعات الجديدة والمهمة في إطار القسم الإجرائي من القانون الجزائي وهو من الموضوعات التي لا تزال بِكرا و لم تنل حظها من البحث والتمحيص على مستوى الفقه الجزائي، إذ أن أغلب الدراسات المنشورة في مجال الجريمة المعلوماتية، اقتصرت على البحث في الجوانب الموضوعية لها دون محاولة الغوص في مسألة إثباتها ومدى تأثير خصائصها على الإجراءات المناسبة في ذلك.

وإذا كانت الجرائم المعلوماتية تعد من الأنماط الإجرامية التي فجرتها حديثا ثورة تقنية المعلومات والإتصالات عن بعد، حيث تعتبر من المستجدات التي لم تكن معروفة للقانون الجزائي سواء الموضوعي أو الإجرائي، فمن دون شك أن أي محاولة للتعامل إجرائيا مع هذا النمط الإجرامي في إطار عملية البحث والتجريب سوف يخلق إشكالات إجرائية للأجهزة المكلفة بهذه العملية، ينبغي أن تأتي الدراسات القانونية عليها بالشرح والتحليل.

ومن هنا تأتي أهمية موضوع البحث الذي حاولت من خلاله مناقشة المفاهيم القانونية المتعلقة بالجرائم المعلوماتية، وربطها بالمفاهيم القانونية المتعلقة بإجراءات تحصيل واستقصاء الدليل

في إثبات الجريمة ، ووضع التصورات والرؤى المتعلقة بالجوانب الإجرائيةفي إطار التعامل مع الجريمة المعلوماتية في ظل النصوص التشريعية الحالية في القانون الجزائري.

أسباب إختيار البحث:

لا يخفى سبب اختياري لهذا البحث، وهو رغبتي في الوقوف على حقيقة التعامل مع الجريمة المعلوماتية من الناحية الإجرائية فالكثير من الدراسات التي عُنيت بهذه الجرائم باتت تركز على الجانب الموضوعي فقط، فوجدت قلة نادرة من المؤلفات ما يتعرض للجانب الإجرائي لذلك حاولت من خلال بحثي هذا إثراء النقاش القانوني حول هذا الموضوع الهام.

أهداف الدراسة:

ينبع الهدف من هذه الدراسة من محاولة المساهمة في وضع الخطوط العريضة للتعرف على طرق التحقيق في هذا النوع من الجرائم، ذلك أن جدة وحداثة الجرائم المعلوماتية وما تتسم به من خصائص سوف يجد معه المحقق نفسه في حيرة أمامها وكيفية التعامل معها وأسلوب التحقيق فيها، إذ لاشك أن إجراءات التحقيق وجمع الأدلة بخصوص هذه الجرائم يختلف عما هو الحال عليه في الجرائم التقليدية.

إشكالية البـــحث:

إذا كانت ظاهرة الإجرام المعلوماتي قد أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي بحثا عن إمكانية تطبيق نصوصه التقليدية على هذا النوع من الجرائم واحترام مبدأ الشرعية والتفسير الضيق للنصوص الجنائية، فقد أثارت في نفس الوقت العديد من المشكلات في نطاق القانون الجزائي الإجرائي، وتبدأ المشكلات الإجرائية في مجال الجرائم المعلوماتية بتعلقها في كثير من الأحيان ببيانات المعالجة الكترونية وكيانات منطقية غير مادية، ومن ثم يصعب الكشف عن تلك الجرائم وإثباتها نظرا للسرعة والدقة العالية في تنفيذها وكذا إمكانية محوها وتمويه آثارها وإخفاء الأدلة المتحصلة منها عقد تنفيذها.

ولذلك فقد امتد تأثير التقنية المعلوماتية إلىالجانب الإجرائي من القانون الجزائي، ذلك أن نصوص هذا القانون إنما صيغت لتحكم الإجراءات المتعلقة بجرائم تقليدية، ترتكب في عالم مادي وملموس يلعب فيه السلوك المادي الدور الأكبر والأهم على خلاف الجريمة المعلوماتية التي ترتكب

في مسرح إلكتروني غير مادي يختلف كليا عن المسرح التقليدي. وهنا يكون التساؤل حول مدى صلاحية هذه الإجراءات لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس. وهل هذا الأمر سوف يجعل من قانون الإجراءات الجزائية قاصرا عن الوفاء بمتطلبات الشرعية الإجرائية في مواجهة هذا النمط الإجرامي، وإذا كان الحال كذلك فإن الوضع يقتضي تدخل المشرع لتعديل قانون الإجراءات الجزائية أو استحداث قانون خاص يضمن توفير القواعد الإجرائية التي يمكن من خلالها لجهات البحث والتحري الوصول إلى الدليل المناسب لإثبات الجريمة المعلوماتية.

فهل استجاب المشرع الجزائري لهذه المبررات واستحدث في سبيل ذلك تشريعات جديدة لمعالجة آثار وانعكاسات التقنية المعلوماتية على إجراءات البحث والتحري، وإلى أي مدى وفق المشرع في استحداث طرق إجرائية في سبيل البحث والتحري عن الجريمة والمجرم المعلوماتي.

وإذ نحن بصدد البحث في هذه الإشكالية الجوهرية تصادفنا تساؤلات يعتبر البحث فيها أمرا ضروريا للإجابة عن جوهر موضوع الدراسة والتي منها:

- ماهي خصائص الجريمة المعلوماتية وكذا خصائص المجرم المعلوماتي، وما مدى تأثيرها على إثبات الجريمة وإسنادها للمتهم؟
- ماهي طبيعة الدليل المناسب لإثبات الجريمة المعلوماتية وماهي خصائصه؟
- كيف يمكن إستخلاص الدليل الرقمي من البيئة الإلكترونية التي يتواجد بها؟
- ماهي الصعوبات والمعوقات التي تواجه جهات البحث والتحري في استخلاص الدليل الرقمي؟
- كيف تعامل المشرع مع هذاالدليل الرقمي في مجال الإثبات الجزائي من حيث كونه دليلا علميا وأثر هذه الخاصية على مبدأ الاقتناع الشخصي للقاضي الجزائي؟
- مامدى حجية المخرجات الإلكترونية في الإثبات نظرا لطبيعتها الخاصة بالمقارنة بوسائل الإثبات التقليدية؟

مــــناهـــج البحث:

وقد تطلب منا هذا البحث إعتمادالمنهج الوصفي كأصل، بالإضافة إلى مناهج أخرى تكميلية وهي المنهج التحليلي ،المقارن ، التأصيلي، نلجأ إليها كلما استوجب منا البحث ذلك.

فالمنهج الوصفي يظهر من خلال قيامنا بوصف ظاهرة الجريمة المعلوماتية وتحديد بعض المفاهيم التي تقوم عليها، وكذا قيامنا بوصف المفاهيم الخاصة بالإجراءات المستعملة في استخلاص الدليل والصعوبات التي تواجهها.

المنهج التحليلي حاولنا في هذا البحث تحليل، بعض المفاهيم والغوص في جزئياتها وطرحها بشكل من التفصيل والتشريح لما بدا لنا من أهميتها، مثلما كان الحال لإجراء تفتيش المنظومة المعلوماتية.

المنهج المقارن نظرا للطبيعة العالمية التي تتميز بها الجريمة المعلوماتية، فإنه ومن دون شك قد نالت حظها من المعالجة التشريعية سواء الموضوعية أو الإجرائية على مستوى التشريعات المقارنة لذلك فقد حاولت في بحثي هذا مقارنة بعض المفاهيم التي أعتمدها المشرع الجزائري مع بعض التشريعاتالأخرى كلما كان ذلك سانحا.

المنهج التأصيلي كان من اللازم في كثير من الأحيان أن نؤصل الأمور ونردها إلى مصدرها رغم ما يكون بشأنها من خلاف فقهي كما هو الحال مثلا بالنسبة للمراسلات الإلكترونية والمراقبة الإلكترونية.

خطة الدراسة:

لقد حاولت أن أحصر نطاق هذه الدراسة ضمن خطة تتكون من فصلين:

قوام الفصل الأول تحليل الجوانب القانونية للجريمة المعلوماتية.

وأما الفصل الثاني فتناولت فيه الجوانب القانونية للتحقيق وإجراءات جمع الدليل في الجريمة المعلوماتية.

الفصل الأول

الجوانب القانــونية للجــريمة المعلومــاتية

بالرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل تقنية المعلومات على جميع الصعد وفي شتى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الإنعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة و الإنحـــراف عن الأغراض المتوخاة منها، تبدت في تفشي طائفة من الظواهر الإجرامية المستحدثة، ألا وهي ظاهرة الجرائـــم المعلوماتية. ليس هذا فحسب بل سهلت هذه التقنية إرتكاب بعض الجرائم التقليـــدية وشكـــلت أرضا خصبة لكثير من الأنشطـــة غير المشروعة المرتبطة بالحاسبات الآليـــة، هـــذه الحاسبات التي أصبحت توفـــر للجناة وسيلة هامة لارتكاب العديد من الجرائم المرتبطة بالمعلـــوماتية ما كانت لتظهر لولا وجود هذه الحاسبات الآلية و ارتباطها بالتقنية المعلوماتية.

ولما كانت الجريمة المعلوماتية ظاهرة إجرامية حديثة نظرا لارتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحاطة هذه الظاهرة بكثير من الغموض، لأجل ذلك فقـــد بدا لي أنه وقبل الخوض في المسائل الشكلية و الإجرائية التي تنطبق على الجريمة المعلوماتية أن أنوه على جانب من القواعـــد الموضوعية لهـــذه الظاهرة الإجرامية، إذ يجب الإلمام بماهية الجرائم المعلوماتية وطبيعتها وإظهـــار موضوعها و خصائصها ومخاطرها وحجم الخسائر الناجمة عنها ودوافع مرتكبيها، وهذا حتما في منظورنا يتخذ أهمية إستثنائية لسلامة التعامل مع هذه الظاهرة من طرف القائمين على مكافحتها.

وعلى ضوء ذلك سأتناول في هذا الفصل تحديد مفهوم الجريمة المعلوماتية و أوجه الحماية الجزائية الموضوعية للنظم المعلوماتية.

المبحث الأول:

ماهيـــة الجريمـــة المعلومـــاتية :

إنه منذ شيوع استخدام الحاسب الآلي أو الكمبيوتر في الستينات ثم السبعينات بدأ الحديث عن بعض الأفعال والسلوكات المرتبطة بالإستخدام غير المشروع للبيانات المخزنة في أنظمة الكمبيوتر والتلاعب بهذه البيانات وتدميرها، وقد رافق ذلك نقاشات وتساؤلات حول ما إذا كانت هذه السلوكات مجرد شيء عابر أم أنها ظاهرة جرمية مستجدة.

ولقد شهد العالم في الفترة الراهنة إزديادًا مطردا في نطاق استخدام تقنية المعلومات وتطورًا بالغا في الإعتماد عليها في تسيير شؤونه، وهو الأمر الذي صاحبه في المقابل ازديادٌ موازٍ للإجرام المعلوماتي.

وتعد الجريمة المعلوماتية من الظواهر الإجرامية الحديثة، وتحديد مفهومها يعد الخطوة الأولى للتعرف على هذه الظاهرة الجرمية من جميع جوانبها القانونية، خاصة إذا علمنا أنه لا يوجد مصطلح قانوني موحد للدلالة على هذه الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر بسبب ذاتيتها وتميزها عن غيرها من الجرائم التقليدية، سواءً في محلها أو خصائصها، ومما لاشك فيه فإن أي محاولة من أجل اختيار وتحديد المصطلح الملائم لهذه الظاهرة ينبغي أن يكون مبنياً ومؤسساً على عدة ضوابط تقنية وقانونية، أولها إدماج البعدين التقني والقانوني، ذلك أن تقنية المعلومات في أصلها هي نتاج اندماج الحوسبة والإتصال، فأما الحوسبة فتقوم على استخدام وسائل التقنية لإدارة وتنظيم ومعالجة المعطيات في إطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق، وأما الاتصال فهو قائم على وسائل تقنية لنقل المعلومات،والضابط الثاني يقوم على أساس البحث بشأن الحدود التي ينتهي عندها العبث وتلك التي تبدأ عندها المسؤولية عن أفعال تعد مجرمة. والضابط الثالث أن يكون اختيار المصطلح شاملا لما يعبر عنه ملما بحدود محله، فلا ينبغي أن يقتصر على الجزء ليعنيَ الكل ولا ينصرف إلى ما لا يجب أن ينطوي تحت نطاقه.

لذلك فلقد بذل المهتمون بدراسة هذا النمط الجديد من الإجرام جهدًا كبيرا من أجل الوصول إلى تعريف مناسب يتلاءم مع طبيعة الجريمة المعلوماتية، ذلك أن عدم الإتفاق على تعريف

هذه الظاهرة الإجرامية إنما يؤدي إلى إثارة عدد من المشكلات العملية يتمثل أهمها في صعوبة تقدير حجم هذه الظاهرة وتعذر إيجاد الحلول اللازمة لمواجهتها، وكذا صعوبة تحقيق التعاون الدولي لمكافحتها.(1)

إلا أن المتفق عليه أن فكرة المعلوماتية هي الفكرة الجوهرية والمركزية في دراسة هذه الظاهرة الإجرامية،ذلك أن المعلوماتية هي شرط مفترض لقيام هذا النوع من الجرائم.

المطلب الأول: مـــــفهوم المعلـــوماتية:

إن المعلوماتية أو ما يسمى أيضا بعلم المعلومات، هو ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها وتخزينها واسترجاعها وتغييرها وكذا تحويلها واستخدامها.(2) كما يهتم هذا العلم بدراسة أساليب معالجة المعلومات كالأنظمة المعلوماتية ونظم البرمجة، وبهذا المفهوم تعتبر المعلوماتية علما متصلا بالعديد من العلوم الأخرى.

وقد صاغت الأكاديمية الفرنسية تعريفا للمعلوماتية بأنها علم التعامل العقلاني بواسطة آلات أوتوماتيكية مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعماداً للاتصالات في ميادين التقنية والاقتصاد والاجتماع.(3)

كما أن منظمة اليونيسكو ذهبت إلى الإدراج في مفهوم المعلوماتية الفروع العلمية والتقنية والهندسية وأساليب الإدارة الفنية المستخدمة في تداول معالجة المعلومات وتطبيقاتها. وقد عرفت التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية المعلوماتية بأنها تشمل الحاسبات الآلية ووسائل الإتصالات وشبكات المعلومات والبيانات والمعلومات التي يمكن تخزينها ومعالجتها واسترجاعها ونقلها بواسطة هذه الحاسبات أو شبكات المعلومات.

لذلك فإنه واسترشادًا بما سبق ذكره من التعريفات التي صيغت لتحديد مفهوم المعلوماتية فإنه يمكن القول بأن مفهومها يقوم أساسا على العلاقة بين المعلومات وبين التقنية الحديثة التي تستخدم

---

(1) نائلة عادل محمد فريد قورة. جرائم الحاسب الالي الاقتصادية .منشورات الحلبي الطبعة الاولى 2005 ص 28.

(2) أحمد خليفة الملط. الجرائم المعلوماتية. دار الفكر الجامعي الاسكندرية. الطبعة الثانية 2006، ص 87.

(3) عقدت هذه الجلسة للأكاديمية بتاريخ 1967/04/6.

في معالجة هذه المعلومات،[1] أو بعبارة أخرى فالمعلوماتية هي المعلومات المبرمجة آليا والتي تستخدمالحاسبات الآلية وبرامجها في التعامل معهالذلك فإنه وللوقوف على تحديد مفهوم المعلوماتية يتطلب منا الأمر أن نستعرض تعريف المعلومات التي تدخل في نطاق الحماية الجزائية في إطار الجريمة المعلوماتية (الفرع الأول) وتحديد خصائصها وطبيعتها (الفرع الثاني) .

الفرع الأول: تعــريف المعلومـــات

تكمن أهمية تحديد المقصود بالمعلومات وكذا طبيعتها في كونها المحل الذي يقع عليه الإعتداء في جرائم المعلوماتية وهو الأمر الذي يقتضي توضيحا دقيقا وفهما عميقا من أجل إصباغ الحماية عليها على نحو صحيح.

ولقد اكتسبت المعلومات بظهور تكنولوجيا الحواسيب بعدًا جديدا أضفى عليها أهمية تفوق ما كانت عليها من قبل، إذ أن المعلومات في الوقت الراهن لم تعد مجرد نوع من الترف تتباهى بها المجتمعات أو المنظمات وإنما أصبحت ركيزة أساسية في تطور المجتمع، سيما بعد أن دخلت تكنولوجيا المعلومات والإتصالات جميع الميادين العلمية الاجتماعية والإنسانية.فعصرنا الحالي والمستقبلي تركز المجتمعات فيه على تعظيم شأن الفكر والعقل الإنساني بعد أن أصبحت المعلومات فيه مصدر قوة اقتصادية وسياسية وعسكرية لارتباطها بمختلف مجالات النشاط الإنساني وتداخلها في كافة جوانب الحياة العصرية، وبات الوعي بأهميتها مظهرًا لتقدم الشعوب والأمم.

وتعرف المعلومات بصفة عامة بأنها "مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل وأشكال مختلفة.[2]

(1)نائلة عادل محمد فريد فورة، المرجع السابق.ص97

(2) مشار إليه لدى د. نائلة محمد فريد فورة. المرجع السابق. ص 97 .

ولقد ذهب البعض إلى القول أنه من الصعب أو من المستحيل وصف المعلومة بدقة وما يمكن فقط هو إدراك أثرها.[1]لذلك فقد اجتهد الباحثون من تخصصات وثقافات مختلفة في وضع تعاريف للمعلومات منها ما أورده الأستاذ « Catala » من تعريف حين اعتبرها أنها "رسالة ما معبر عنها في شكلٍ يجعلها قابلة للنقل أو الإبلاغ للغير."[2]كما عرفت أيضا بأنها "النقل المجرد لوقائع معينة تم الحصول عليها من مصادر متعددة"[3].

ورغم المحاولات المتعددة نحو وضع نص قانوني يتكفل بوضع تعريف محدد للمعلومة فإنه لحد الآن لا يوجد تعريف مانع بنص قانوني.

ومع ذلك فقد أشار المشرع الفرنسي وفقا للقانون رقم 652/82 الصادر في 1982/07/26 الخاص بالاتصالات السمعية والبصرية إلى المعلومة على أنها "صور الوثائق والبيانات والرسائل من أي نوع"

وفي هذا الإطار عرف المشرع الأمريكي المعلومات في قانون المعاملات التجارية الإلكترونية لسنة 1999 بالمادة الثانية الفقرة العاشرة منه بأنها "تشمل البيانات والكلمات والصور والأصوات والرسائل وبرامج الكمبيوتر والبرامج الموضوعة في الأقراص المرنة وقواعد البيانات أو ما شابه ذلك".

كما عرفها القرار الصادر بتاريخ 22 ديسمبر 1981 المتعلق بإثراء المصطلحات المعلوماتية في فرنسا بأنها "تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير بفضل علامة أو إشارة من شأنها أن توصل المعلومة لهذا الغير".

ومن القوانين العربية التي عرفت المعلومات القانون الاتحادي لدولة الإمارات العربية المتحدة رقم (1) لسنة 2006 المتعلق بالمعاملات التجارية الإلكترونية في مادته الأولى بنصه على أنها بيانات ومعلومات إلكترونية في شكل نصوص أو رموز أو أصوات أو رسوم أو صور أو برامج الحاسب الآلي أو غيرها".

(1) أحمد أنور بدر .الإتصال العلمي، دار الثقافة العلمية، القاهرة، د.ت ص 17 .

(2) رشيدة بوكر.جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري و المقارن.منشورات الحلبي الحقوقية الطبعة الأولى 2012 ص.65

(3) خالد ممدوح ابراهيم أمن الجريمة الالكترونية، الدار الجامعية 2008 ص 27.

كما عرفها في القانون رقم (2) لسنة 2006 في شأن مكافحة جرائم تقنية المعلومات بأنها كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنية المعلومات وبوجه خاص الكتابة والصور والصوت والأرقام والحروف والرموز والإشارات وغيرها."

وقد عرف القانون الأردني للمعاملات الإلكترونية رقم 85 لسنة 2001 في المادة الثانية منه المعلومات بأنها "البيانات أو النصوص أو الصور أو الأشكال أو الأصوات أو الرموز أو برامج الحاسوب أو قواعد المعلومات التي أنشئت أو أرسلت أو استلمت أو خزنت بوسائل إلكترونية".

وعرف قانون البحرين رقم 83 لسنة 2002 المتعلق بالمعاملات الإلكترونية المعلومات بأنها "البيانات والصور والنصوص والأصوات والرموز وبرامج الحاسوب والبرمجيات ويمكن أن تكون قواعدالبيانات والكلام".

ويتبين من التعريفات السابقة أنها أعطت مفهوما موسعاً للمعلومات من خلال إضافتها لعبارة "من أي نوع" كما في تعريف القانون الفرنسي أو بعبارة ما شابه ذلك كما في تعريف القانون الأمريكي، وهذا ربما تحسباً لما قد يظهر من أشكال جديدة للمعلومات وذلك لارتباطها بتقنية الحاسوب والتطور التكنولوجي الذي قد تظهر معه وسائل أخرى تنقل بواسطتها المعلومة.

أولا: الفــرق بين المعلــومات والمعــطيات:يميز الكثير من الدارسين والباحثين في هذا المجال عند تعريف المعلومات بينها وبين المعطيات،[1] فهذه الأخيرة تعبر عن مجموعة من الأرقام والكلمات والرموز أو الحقائق أو الإحصاءات الخام التي لاعلاقة بين بعضها البعض و لم تخضع بعد للتفسير أو التجهيز للإستخدام، أما المعلومات فهي المعنى الذي يستخلص من هذه المعطيات. [2]

وقد عرفت الوكالة الفرنسية للتقييس(Afnor)المعطيات (Les donnés) بأنها كل حادث مفهوم أو تعليمة تقدم في شكل متفق عليه قابلة للتبادل عن طريق البشر أو بواسطة الحاسوب أو

([1]) المعطيات في اللغة تعني البيانات لذلك نجد الكثير من الكتب يستعمل فيها هذا المصطلح بدل مصطلح المعطيات. ويقابلها في الفقه اللاتيني كلمة (Dattum) وتعني شيء معطى أو مسلم به أو شيء ما معروف أو مسلم بصحته ,بينما تستخدم في اللغة الفرنسية مقابلا لها كلمة (Données).

([2]) هشام محمد فريد رستم. قانون العقوبات ومخاطر تقنية المعلومات.مكتبة الآلات الحديثة 1992، ص 26.

ينتجها الحاسوب.[1]ولقد اعتمدت إتفاقية بودابست للجريمة المعلوماتية في تعريف المعطيات ذات التعريف الذي ذهبت إليه هيأة التوصيف العالمية الإيزو، حيث نصت في مادتها الأولى على أن "المعطيات هي كل تمثيل للوقائع أو للمعلومات أو المفاهيم تحت أي شكل وتكون مهيأة للمعالجة بما في ذلك برنامج معد من ذات الطبيعة ويجعل الحاسب يؤدي المهمة". وقد أخذت التوصية الصادرة عن منظمة التعاون الإقتصادي والتنمية في 1992/11/26 الخاصة بحماية أنظمة الحاسبات الآلية وشبكات المعلومات بالتفرقة السابقة، حيث عرفت المعطيات بأنها مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلا محددًا يجعلها قابلة للتبادل والتغيير أو للمعالجة بواسطة الأفراد أو بوسائل إلكترونية، أما المعلومات فهي المعنى المستخلص من هذه المعطيات.

وتأسيساً على هذا المعنى فإن المعطيات تعتبر المواد الخام التي تستخرج منها المعلومات باستخدام[2] معالجة آلية في عملية الإستخراج، إذ يتم تجميع وتشغيل المعطيات للحصول على المعلومات ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من المعطيات والتي يحصل تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية،[3] وهي ميزة تتميز بها المعلومات من خلال قابليتها للدمج، فقد تضاف معلومةٌ إلى معلومةٍ أخرى ليكونا معاً معلومة جديدة تختلف في قيمتها وأهميتها، وبالتالي في مقدار الحماية اللازمة لها.[4]وهو ما يطلق عليه النظرية التكاملية للمعلومات، ومن هذا المنطلق يتضح جلياً أن المعطيات هي المعلومات في حالة سكون وأن المعلومات هي المعطيات في حالة معالجة. وبهذا التصور تكون المعطيات عبارة عن حقائق رقمية أو غير رقمية تتم بطريقة منهجية يمكن فهم دلالتها مباشرة دون الدخول في عمليات إستنتاجيةإستقرائية لدلالتها المعقدة من خلال الربط بين أكثر من بيان منها،[5] لأن ذلك يعني

([1]) مفتاح محمد دباب، معجم المصطلحات وتكنولوجيا المعلومات والاتصالات. الدار الدولية للنشر .القاهرة 1995 ص 42.

([2]) يدلل البعض على هذه التفرقة بالمثال التالي: إن عبارة « Le soleil brille » باللغة الفرنسية تعني أن الشمس مشرقة وهي لا تعدو أن تكون بيانا لحالة الشمس ولا يمكن أن تتحول إلى معلومة لدى الأشخاص إلا إذا توافر شرطان: الأول أن يطلع عليها بالفعل، والثاني أن يكونوا على علم باللغة الفرنسية حتى يتمكنوا من فهمها وحتى يتحقق هذان الشرطان تضل المعطيات مجموعة من الحروف ولا يمكن أن تتحول إلى معلومة إلا بتوافرهما.

([3]) انتصار غريب أمن الكمبيوتر والقانون. دار الراتب الجامعية بيروت .ص 81 .

([4]) على سبيل المثال رقم حساب عميل في البنك معلومة على قدر من الأهمية وتحتاج إلى حمايتها إلا أنه إذا أضفنا إلى هذه المعلومة معلومة أخرى كإسم العميل وإسم البنك وحجم الرصيد فإن قيمة المعلومة وأهميتها في هذه الحالة تتضاعف وتتطلب قدرا أكبر من الحماية.

([5]) رشيدة بوكر المرجع السابق، ص 67.

التحول من كون الأمر مجرد معطيات إلى معلومات، فالمعلومات وفقا لذلك هي النتيجة المبدئية أو النهائية المترتبة على تشغيل المعطيات وتعليلها أو استقراء دلالتها واستنتاج ما يمكن استنتاجه منها وحدها أو مترافقة مع غيرها أو تفسيرها على نحو يثري معرفة مستخدمي القرار ويساعدهم في الحكم السديد على الظواهر والمشاهدات أو يسهم في تطوير المعارف النظرية أو التطبيقية.(1)(2)

والمشرع الجزائري على غير العادة عمد إلى وضع تعريف للمعطيات بموجب المادة الثانية من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها بنصه في الفقرة ج من هذه المادة على أن المعطيات المعلوماتية هي أي عملية عرض للوقائع أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

ثانيا: الفـــرق بين المعلـــومات والبرامـــــج :يعتبر البرنامج من العناصر الرئيسية للكيان المنطقي لأي حاسوب، ومن دونه يصبح هذا الأخير (الحاسوب) مجرد مجموعة من معدات وآلات صماء.(3) وقد نال برنامج الحاسوب حظه من التعريفات العلمية والقانونية فتعددت وتباينت بين مضيق لمدلوله وموسع له، ومن هذه التعريفات العلمية للبرنامج أنه مجموعة من الأوامر والإرشادات والإيعازات التي تحدد لجهاز الحاسوب العمليات التي يقوم بتنفيذها بتسلسل وخطوات محددة، وتُحمل هذه العمليات على وسيط معين يمكن قراءته عن طريق الآلة، وبعد ذلك يمكن للبرنامج عن طريق معالجة المعطيات أن يؤدي وظائف معينة ويحقق النتائج المطلوبة(4).

كما عُرف أيضا أنه مجموعة من التعليمات المتتابعة بصفة منطقية توجه إلى الكمبيوتر لأداء العمليات المنطقية المطلوبة(5).

---

(1) محمد محمد شتا. فكرة الحماية الجنائية لبرنامج الحاسب الآلي، دار الجامعة الجديدة للنشر 2002، ص 61.

(2) ويجد المصطلحان المعطيات ولمعلومات فرقا فنيا بينهما فالمعطيات (Data) هي المدخلات in Put إلى جهاز الكمبيوتر بهدف تشغيلها ومعالجتها داخل الجهاز، والمعلومات هي المخرجات « Out put » بعد عملية المعالجة.

(3) عفيفي كامل عفيفي. جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة- منشورات الحلبي الطبعة02، 2007، ص 25.

(4) محمد بلال الزعبي. أد أحمد الشرايعة منيب قطيشات، مهارات الحاسوب البرمجيات. دار وائل للنشر الطبعة الخامسة عمان ص 36.

(5) انظر في هذا المعنى محمد محمد الهادي، تكنولوجيا المعلومات وتطبيقاتها، الطبعة الأولى دار الشروق، القاهرة 1989 ص 110.

ووفقا للمفهوم العلمي للبرامج فإنها تصنف إلى قسمين: برامج النظام وبرامج التطبيقات، فأما الأولى فإنها تقوم بوظيفة إجرائية حيث تسيطر على العمليات الأساسية الأولى داخل الكمبيوتر وأما الثانية فهي برامج مصممة من أجل أداء وظائف معينة تستجيب لاحتياجات العملاء ومتطلباتهم[1].

ومن التعريفات القانونية للبرنامج أنه: "مجموعة من التعليمات الموجهة من الإنسان إلى الآلة والتي تسمح بتنفيذ مهمة معينة".[2] وقد عرفت المنظمة العالمية للملكية الفكرية المعروفة باسم "الريبو" البرنامج بأنه "مجموعة من التعليمات التي تسمح بعد نقلها على دعامة مقروءة من قبل الآلة بيان أداء أو إنجاز وظيفة أو مهمة أو نتيجة معينة عن طريق آلة قادرة على معالجة المعلومات.

وعلى نفس المفهوم درَج المشرع الأمريكي من خلال القانون الصادر سنة 1980 الخاص بحماية حق المؤلف إلى تعريف البرنامج (Software) بأنه مجموعة توجيهات أو تعليمات يمكن للنظام استخدامها بشكل مباشر أو غير مباشر للوصول إلى نتيجة معينة. أما الحال في فرنسا فإن المشرع الفرنسي لم يتجه إلى وضع تعريف للبرنامج سواء من خلال النصوص الجزائية التي تنظم الجرائم محل الدراسة أو في إطار القانون رقم 85/690 المؤرخ في 1985/07/3 المتعلق بحقوق المؤلف، إلا أن القرار الوزاري الصادر عن وزير الصناعة والتعليم الوطني في 1982/11/22 بخصوص إثراء اللغة الفرنسية، فقد عرف البرنامج على أنه مجموعة الخطوات والإجراءات التي تهدف إلى تشغيل نظام متكامل لأنظمة المعالجة المعلوماتية وتوظيفها وفقا لهذا الغرض الذي من أجله تم وضع هذا البرنامج.

ومن الواضح أن المشرع الجزائري قد واكب الإتجاه الذي سلكته أغلب التشريعات في معظم الدول حينما أدمج في القانون 05/03المتعلق بحقوق المؤلف والحقوق المجاورة المصنفات المعلوماتية ضمن قائمة المصنفات الأصلية المحمية والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي حيث نصت المادة الرابعة الفقرة أعلى أنه "تعتبر على الخصوص كمصنفات أدبية أو فنية محمية:

---

(1) رشيدة بوكر، المرجع السابق، ص 69.

(2) عماد محمد سلامة، الحماية القانونية لبرنامج الحاسب الآلي ومشكلة قرصنة البرنامج الأول، دار وائل للنشر، عمان 2005، ص 48.

أ- المصنفات الأدبية المكتوبة مثل....برامج الحاسوب...." كما تضمنت الفقرة الثانية من المادة 05 قواعد البيانات بنصها: "تعتبر أيضا مصنفات محمية الأعمال الآتية:

- المجموعات والمختارات من المصنفات.... وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى".

والملاحظ أن المشرع الجزائري قد اكتفى فقط بإدماج برامج الحاسوب ضمن المصنفات الأصلية المحمية دون الخوض في تحديد مفهوم البرنامج، وهذا راجع ربما لتعقد فكرة البرامج ذاتها بسبب ارتباطها بتطور تكنولوجيا نظم المعلوماتية واستخداماتها مما يصعب حصرها في نطاق محدد.

هذا وإن كان بعضٌ من الفقه يرى جدوى من التمييز والتفرقة بين المعطيات والمعلومات والبرامج إلا أنه وفي الإتجاه المعاكس يرى جانب آخر من الفقه عدم وجود أهمية في التمييز بينها،[1] طالما أن المعلومات هي المعنى المستخلص من المعطيات بعد معالجتها وأن البرنامج هو المستودع الذي يتم فيه معالجة هذه المعطيات، فالعلاقة بينها إذن هي علاقة الجزء بالكل.ولما كانت الغاية في المقام الأول هي حماية المعلومات فالكل يتمتع بنفس الحماية القانونية في إطار الجرائم المعلوماتية طالما أن هذه المعلومات موجودة داخل بيئتها الإلكترونية[2].

ولقد نحا المشرع الجزائري هذا المنحى حينما أدرج برامج الحاسوب ضمن مفهوم المعطيات و لم يأبه لهذا الجدل الفقهي من حيث التمييز بينها، حيث نصت المادة الثانية من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال في تعريفها للمعطيات أن هذه الأخيرة هي "أي عملية عرض للوقائع أو المعلومات.بما في ذلك البرامج المناسبة التي من شانها أن تجعل المنظومة المعلوماتية تؤدي وظيفتها".

(1) نائلة محمد فريد فورة. المرجع السابق. ص 98.

(2) يتحدد نطاق الحماية الجزائية للمعلومات أن تكون في شكلها الإلكتروني فحسب ليخرج بذلك من نطاقها المعطيات التي لم تعالج بعد و لم تدخل في نظام المعالجة، وكذلك المعلومات التي تم معالجتها ثم انفصلت عن بيئـــتها الالكترونية وسجلت على شيء مادي وأصبحت خارج النظام. وهذا ما أشارت اليه المذكرة التفسيرية لاتفاقية بودابست في إطار توضيحها لمعنى المعلومات عندما أشارت إلى أنه يجب فهمها على أنها معلومات تأخذ شكلا إلكترونيا أو أي شكل آخر يسمح لمعالجتها مباشرة.

ولعل السؤال الذي يطرح نفسه في هذا الصدد هل كل ما يحتويه النظام المعلوماتي من معلومات تصلح لأن تكون محلا للجريمة المعلوماتية ومن ثم إصباغ الحماية الجزائية من الاعتداء عليها؟

الفرع الثاني: خصـــائص وشـــروط المعـــلومة

إنه بالنظر إلى المعلومة كنتاج للنشاط الفكري الإنساني فقد ذهب الفقه القانوني إلى تقسيم المعلومات[1] إلى ثلاث طوائف:

الطائفة الأولى: المعلومات الإسمية وهي بدورها تنقسم إلى مجموعتين وهي المعلومات الشخصية[2] والمعلومات الموضوعية، فأما الشخصية فالمقصود بها تلك المعلومات المرتبطة بالشخص المخاطب بها كإسمه وحالته الاجتماعية وموطنه وكل ما يكون مرتبطا بشخصه.ومن الطبيعي أن ترد هذه المعلومات في غير حالة الأشخاص الطبيعيين على ممثلي الشخص المعنوي،[3] ولا يجوز للغير الإطلاع عليها إلا بموافقته الشخصية أو بأمر أو إذن من السلطات المختصة.

([1]) عبد الله علي محمود. سرقة المعلومات المخزنة في الحاسب الآلي. دار النهضة العربية، ص 159.

([2]) لقد لقيت مسألة حماية المعلومات الشخصية في جعل تقنية المعلومات إهتماما واسعا على مستوى التنظيم الدولي وكذا على مستوى التشريعات الوطنية، ففي عام 1968 شهد مؤتمر الأمم المتحدة لحقوق الإنسان طرح موضوع مخاطر التكنولوجيا على الحق في الخصوصية.كما أنه وعلى مستوى التشريع المقارن فقد حرص المشرع الفرنسي على حماية المعلومات الشخصية وذلك بموجب القانون 17/78 المؤرخ في 1978/01/06 والخاص بالمعالجة الإلكترونية للمعلومات الإسمية وإعمالا منه لهذا المبدأ ونظرا لخطورة ما يترتب على معالجة المعلومات الاسمية من تهديد لخصوصيات الأفراد، فقد أحالت المواد (41-44) والمادة 46 من القانون 17/78 المذكور أعلاه المعدلة بالقانون 1994/1336 المؤرخ في 1992/12/16 إلى المواد 226-16 إلى 226-24 من قانون العقوبات بشأن الجرائم التي تقع بمخالفة أحكام القانون 17/28 المتعلق بحماية الأفراد من مخاطر المعالجة الآلية للمعلومات الاسمية.

وقد أشارت الدراسة الصادرة عن مجلس الدولة الفرنسي حول الإنترنت والشبكات الرقمية في 1998/07/02 إلى الموضوعات الهامة الواجبة الحماية وقد كان في مقدمتها ضرورة حماية المعلومات الشخصية والحياة الخاصة على الشبكات والتي تعد إحدى المسائل الأكثر حساسية في نظر المستخدمين، وقد خلصت الدراسة في توصياتها إلى أن حماية المعلومات الشخصية أصبحت مهددة إزاء مخاطر جديدة في بنية الشبكات الرقمية.

([3]) الشحات ابراهيم منصور، الجرائم الالكترونية، دار الفكر الجامعي الطبعة الأولى، ص 25.

وأما المعلومات الموضوعية فهي تلك المعلومات المنسوبة لشخص آخر وتكون موجهة للغير ولا تتعلق بشخص صاحبها ويمكن إدلاء الغير برأيه الشخصي فيها. ومثالها المقالات الصحفية والملفات الإدارية[1].

الطائفة الثانية: المعلومات الخاصة بالمصنفات الفكرية: وهي عبارة عن معلومات تكون غالبا محمية بتشريعات الملكية الفكرية، ويتمتع أصحابها بحق الإستئثار بها وبحقوق مالية وأدبية عليها.

الطائفة الثالثة: المعلومات المباحة: ويقصد بها المعلومات التي يباح للجميع الحصول عليها دون إذن، لأنها بدون مالك[2] ومثالها تقارير البورصة أو النشرات الجوية، وتنعقد ملكية هذه المعلومات إلى من قام بجمعها وصياغتها.

وإذا كان الغرض من الإعتداء على النظام المعلوماتي هو المعلومة فهل ينبغي أن تظهر في إطار معين وتتميز بخصائص معينة تكون جديرة بالحماية؟.

أولا: الخصـــائص الممـــيزة للمعـــلومات: تتميز المعلومات بصفة عامة بمجموعة من الخصائص التي تساعد على التعرف على طبيعتها وأهميتها وعلى مقدار الحماية اللازمة لها، وتنقسمهذه الخصائص إلى طائفتين، الأولى وهي الخصائص الأساسية والثانية هي الخصائص التكميلية.

1/الخصائص الأساسية أو الأولية للمعلومـــة: تستند المعلومة في أصلها على أربع أركان رئيسية وهي نوع المعلومة، الصورة التي توجد عليها المعلومة، شكل المعلومة، والوسيط الذي توجد عليه المعلومة.

فالمعلومات تختلف فيما بينها من حيث النوع، وتبعا لذلك تختلف أهميتها، فقد تكون المعلومة نوعا من المعرفة، وقد تكون في شكل رسم هندسي وقد تتخذ شكل مجموعة من الأوامر والتعليمات،[1]

([1]) أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي دراسة مقارنة دار النهضة العربية، ص 202 وما بعدها

([2]) خالد ممدوح ابراهيم. المرجع السابق .ص 30.

وقد تتعلق بأمور مالية أو بأمور ذات طبيعة فنية أو غير ذلك من الأشكال التي قد توجد المعلومة عليها.

ولا يقتصر الإختلاف على نوع المعلومة فقط وإنما يمتد أيضا إلى الصورة التي توجد عليها، فلا تظهر المعلومات في صورة واحدة بل تتعدد صورها، فقد تكون داخل نظام المعالجة الآلية أو في حالة حركة من نظام إلى آخر، كما أنها قد تكون مقروءة أو مسموعة. وتتوقف قيمة المعلومة والحماية اللازمة لها في كثير من الأحيان على الصورة التي تكون عليها.

لذلك تقتضي حماية المعلومات الحفاظ عليها في كل صورة توجد عليها، وكذا حماية البرامج المسؤولة على تحويل المعلومات من صورة إلى أخرى كلما اقتضى الأمر. خاصة إذا كانت المعلومة متحركة وتنتقل عبر شبكات الإتصال، ففي رحلتها عبر الشبكات تكون عرضة للكثير من المخاطر،[2] فقد تتغير الصورة التي توجد عليها المعلومة بسبب التلاعب بها، فإدخال أحد البرامج الخبيثة إلى الحاسب الآلي من شأنه أن يغير من صورة المعلومة على نحو سلبي قد يؤدي إلى تحويل المعلومة على الشاشة إلى مجموعة من الحروف المبعثرة. كما قد يقوم هذا البرنامج الخبيث (الفيروس) بتغيير صورة المعلومات في ذاكرة الحاسوب إلى خليط من الحروف[3].

- أما عن شكل المعلومة فيقصد به في مجال المعلوماتية الطريقة التي تكتسب بها المعلومات من خلال الحاسب الآلي، كأسلوب كتابة البرنامج والقواعد والرموز والكلمات المستخدمة في كتابته بالإضافة إلى القواعد اللغوية التي تتعلق بترتيب الكلمات والعناصر المكونة للتعليمات في لغة البرمجة

([1]) يكتسب هذا النوع من المعلومات أهمية وقيمة نظرا لاستخدامها في مجالات الحاسبات الآلية فالمعلومة في هذه الحالة تتخذ شكل برامج الحاسب الآلي (Software) تعطي التعليمات اللازمة لتشغيل الحاسب الآلي وقيامه بالعمليات المطلوبة منه. ومن ثم كانت هذه البرامج وسيلة لارتكاب كثير من جرائم المعلوماتية، ولا يختلف الأمر سواء كانت هذه البرامج مصدرية أم برامج هدف. وهما نوعان من البرامج تستخدم لتشغيل الحاسب الآلي. فبرنامج المصدر يعتبر بمثابة معلومات مقروءة لمستعمل الحاسب بينما برنامج الهدف يعتبر بمثابة معلومات مقروءة للحاسب نفسه تمكنه من إنجاز التعليمات الموكولة له وذلك من خلال قيام الحاسب الآلي بترجمة برنامج المصدر إلى اللغة التي يفهمها عن طريق الهدف. وفي كلتا الحالتين يمكن التلاعب بالبرنامج وتغييره وإن كانت لا توجد صعوبة كبيرة في اكتشاف التلاعب الذي قد يلحق ببرامج المصدر فعلى العكس من ذلك، فيما يخص برامج الهدف إذ يصعب اكتشاف التلاعب الذي قد يلحق بهذا النوع من البرامج دون مقارنة دقيقة مع نسخة أخرى من نفس البرنامج.

([2]) حسن طاهر داوود. جرائم نظم المعلومات. أكاديمية نايف العربية للعلوم الأمنية الرياضالطبعة الأولى 2000، ص 174.

([3]) نائلة محمد فريد فورة، المرجع السابق، ص 102.

وقواعد التشفير التي تحدد طريقة تمثيل المعلومات بالشفرة بحيث يمكن فك هذه الشفرة فيما بعد لقراءة محتوى هذه المعلومات.

ولابد أن يمتد نطاق حماية المعلومات إلى القواعد المتصلة بشكلها من أجل منع التلاعب بالمعلومات عن طريق المساس بهذه القواعد. ذلك أن أي تغيير يمكن أن يطرأ على شكل المعلومة قد يترتب عليه تغير في معناها أو فقدانها تماما. كأن يقوم أحد الأشخاص بتشفير جميع النسخ المتعلقة بملف معين ثم يقوم بتغيير قواعد التشفير المسؤولة عن فك الشفرة فتصبح المعلومة بهذا الشكل عديمة القيمة[1].

(1) نائلة محمد فريد قورة، المرجع السابق، ص 107.

والمعلومات بطبيعتها تتطلب وجود وسائط تخزن فيها في الحاسبات الآلية، ولاشك أن التلاعب الذي قد يقع على هذا الوسيط من شأنه تعريض المعلومات للخطر.

2/الخصـــائـــص التكميلـــية للمعلـــومات:إنه للوقوف على طبيعة المعلومة وبالتالي التعرف على نوع الحماية اللازمة لها قد يتم الإستعانة ببعض الخصائص التكميلية والتي تتمثل أساسا في مدى إتاحة المعلومة، مدى أهمية المعلومة، مقدار ما تعطيه من فائدة، مقدار ما تتمتع به المعلومة من صحة ومصداقية، معرفة وتحديد مالك المعلومة أو من يسيطر عليها وكذا تحديد المكان الذي توجد به المعلومة وقيمتها من حيث الزمان، وذلك من خلال الوقوف على ما إذا كان للمعلومة قيمة في وقت معين أم تتناقص وتنتهي بانتهاء هذا الزمن بالإضافة إلى معرفة موضوع المعلومة والأثر الذي تحدثه عند معرفتها.

وفي الأخير فإن كل هذه الخصائص والسمات التي تتمتع بها المعلومة سواء الأساسية أو التكميلية تساعد في التعرف على طبيعة المعلومة ومن ثم تقدير قيمتها بغية الوقوف على درجة الحماية اللازمة لها.

ثانيا: الشـــروط الواجب توافرها في المعلـــومة: لكي تكتسب المعلومة قيمة تجعلها جديرة بتوفير الحماية لها لابد أن تستوفي شروطاً نحاول أن ندرسها بشيء من التفصيل فيمايلي:

1)إن يتوافر في المعلومة التحديد والإبتكار: إذا كانت المعلومة هي تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ والتبادل عن طريق علامات أو إشارات مختارة، فينبغي أن تكون محددة من خلال حصرها في دائرة خاصة بها وتحديد جوانبها، ذلك أن المعلومة التي تفتقر لصفة التحديد لا يمكن أن تكونمعلومة حقيقية، لأن الاعتداء يجب أن ينصب على شيئ محدد وأن يكون هذا الشيءمحلا لحق محدد .أما شرط الإبتكار فهو صفة أساسية في المعلومة تنصب على الرسالة التي تحملها المعلومة، فالمعلومة غير المبتكرة هي معلومة عامة ومتاحة للجميع ولا يمكن نسبتها لشخص محدد

2)أن يتوافر في المعلومة السرية والإستئثـــار: إن صفة السرية تجعل من المجال الذي تتحرك فيه المعلومة محصورًا ومحددا بمجموعة معينة من الأشخاص. وإذا انعدم هذا الحصر أصبحت

المعلومة غير سرية وقابلة التداول وهي بذلك بمنأى عن أي حيازة، كالمعلومات المتعلقة بحدث معين أو بحقيقة معينة فهي معلومات تفتقر إلى السرية ولا يمكن أن تكون محلا يعتدى عليه.

وتكتسب المعلومة سريتها بالنظر إلى طبيعتها أو بالنظر إلى رغبة صاحبها أو للأمرين معا ولاشك أن القيمة الاقتصادية ترتبط بالسرية لأن قيمتها تنخفض كلما زاد عدد العارفين بها، كما ترتبط بمدى سهولة أو صعوبة حصول الغير عليها بوسائله الخاصة، والطابع السري للمعلومة يحدد نطاق استعمالها في دائرة محددة ويقلل من استخدام المعلومة ويقصرها فقط على دائرة المؤتمنين عليها الذين يجدون أنفسهم منتفعين بحق الإستئثار عليها(1).

ويتوافر للمعلومة صفة الإستئثار إذا كان الوصول إليها غير مصرح به إلا لأشخاص محددين غالبا ما تكون لمن له سلطة على المعلومة وحق التصرف فيها، وذلك نتيجة وجود نوع من الرابطة تتحقق عندما يكون موضوع هذه المعلومة فكرة أو عملا ذهنيا فتنشأ رابطة بين المعلومة ومؤلفها باعتبارها ملكا خاصا به. وقد تتحقق أيضا هذه الرابطة حتى ولو انصب موضوع المعلومات على بيان حقيقة أو واقعة ما، فهذا النوع من المعلومات هو في الأصل غير سري ومتاح للجميع، ولكن إذا قام شخص بتجميع وحفظ هذه المعلومات ذاتها فهو ينشئ عن طريق هذا التجميع والحفظ معلومة جديدة له أن يستأثر بالتصرف فيها.

المطلبالثاني: تعريف الجريمة المعلوماتية

إن الجرائم الناشئة في البيئة الرقمية جرائم حديثة، ارتبط مفهومها ولا يزال يرتبط بتكنولوجيا الحاسبات وتطوراتها المستخدمة في تشغيل وتخزين ونقل المعلومات في شكل إلكتروني، وكذا بتكنولوجيات وسائل الإتصال وشبكات الربط، لذلك فإنه من الضروري أن يكون أي تعريف لهذا النمط من الجرائم متسماً بالمرونة بما يسمح باستيعابه وتواكبه مع سائر التقنيات المبتكرة الراهنة والمستقبلية في مجال تكنولوجيا التعامل مع المعلومات.

لكن التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حال دون وضع تعريف فقهي جامع وشامل لمفهوم الجريمة المعلوماتية(2) خشيةً من حصر نطاقها داخل إطار تجريمي محدد قد يضر

(1) خالد ممدوح ابراهيم، المرجع السابق ص 31.

(2) خالد ممدوح ابراهيم، الجرائم المعلوماتية الدار الجامعية، ص 73

بها خاصة في ظل التطور المستمر للتقنية المعلوماتية، فما يتم تجريمه اليوم قد يصبح غير ذي أهمية بالنسبة لصور مستحدثة أخرى تظهر نتيجة استخدام تقنيات جديدة.

وإذا كان التطور المتجدد والمستمر للمعلوماتية يمنع صور التجريم الحالية عن مواكبة ما يطرأ من صور إجرامية مستحدثة في مجال المعلوماتية إلا أن وضع قواعد قانونية تنظم أوجه الحماية الجنائية أفضل بكثير من ترك ما يستجد على الساحة الجنائية دون حماية، وهذا ما يقع على عاتق الفقه بداية بوضع تعريف لهذه الظاهرة الإجرامية،و الذي قد يسهم في صياغة المشرع للنصوص القانونية ويساعد القضاء في تفسير هذه النصوص وتكييف الوقائع.

ولقد ذهب الفقهاء في تعريف الجريمة المعلوماتية مذاهب شتى ووصفوا تعريفات مختلفة تتمايز وتتباين تبعا لموضوع العلم المنتمية إليه وتبعا لمعيار التعريف ذاته. فاختلفت بين أولئك الباحثين في الظاهرة الإجرامية الناشئة عن تقنية المعلوماتية من الوجهة التقنية، وأولئك الباحثين في ذات الظاهرة من الوجهة القانونية. وحتى من الوجهة القانونية تعددت التعريفات واختلفت بحسب الدراسة القانونية التي تتناولها1(2).

وفي سبيل ذلك فإن الفقه الجنائي قد بذل محاولات عديدة لتعريف الجريمة المعلوماتية،ولعل جميع المحاولات التي بذلت من أجل تعريف الجريمة المعلوماتية لا تخرج عن أحد الإتجاهين أولها يضيق من مفهومها والثاني يوسعه.

الفرع الأول: الإتجاه الذي يضيق مفهوم الجريمة المعلوماتية:

يذهب أنصار هذا الاتجاه إلى حصر الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، وأن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة تعد جرائم عادية

(2)ذلك أن الجريمة المرتكبة بواسطة تقنية المعلومات تدخل في نطاق دراسات القانون الجنائي الوطني والتي تقع في صميم القسم الخاص لقانون العقوبات، وأنها من الجرائم التي تتخطى حدود الدولة الواحدة فهي تدخل أيضا في نطاق دراسات القانون الجنائي الدولي، ونظرا لنمو وتزايد التجارة الإلكترونية من خلال المبادلات والمراسلات التجارية الإلكترونية فإن الجرائم المرتكبة بواسطة تقنية المعلومات لصيقة الصلة بالقانون التجاري وبحركة التجارة العالمية الحديثة،كما أن الإستعمال الواسع لتقنية المعلومات في المجتمع مكنت من تخزين و استرجاع وتحليل كميات هائلة من البيانات الشخصية فخلقت بذلك سلسلة من التحديات الجديدة و التهديدات الخاصة بالحياة الشخصية وأدى ذلك إلى تزايد انتهاك الحقوق الأساسية و الحريات الفردية التي كفلتها القوانين الدستورية مما يدل على ارتباط الموضوع أيضا بالقانون الدستوري وارتباطه في نفس الوقت بالقانون الإداري خاصة في ظل ظهور وبروز الحكومات الإلكترونية

تتكفل بها النصوص التقليدية للقوانين العقابية، وذلك على خلاف الجرائم التي يتوافر لها هذه المعرفة فهي فقط التي تكون بحاجة إلى نصوص خاصة تتلاءم مع طبيعتها التي تختلف عن غيرها من الجرائم التقليدية.[1]

ومن التعريفات التي وضعها أنصار هذا الإتجاه أن الجريمة المعلوماتية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية ولملاحقته وتحقيقه من ناحية أخرى،[2]وفي هذا الإتجاه أيضا عرفها الفقيه David Thomson(دافيدتومسون) أنها أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب.[3]

وحسب هذا التعريف فإنه يشترط أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة من العلم بتكنولوجيا الحاسبات، وهذا المفهوم قد أخذت بها وزارة العدل الأمريكية في تقريرها الصادر عام 1989 بعد تبنيها لدراسة وضعها معهد ستانفورد الدولي للأبحاثحينما عرف الجرائم المعلوماتية بأنها أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها.

وفي هذا الإتجاه أيضا عرفها جانب من الفقه بالنظر إلى معيار نتيجة الإعتداء، إذ يرى الأستاذ MASS أن المقصود بالجريمة المعلوماتية هي تلك الإعتداءات التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح .كما عرف الأستاذ PARKER الجريمة المعلوماتية بأنها كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنها خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل.

وهناك جانب آخر أخذ في تعريفه للجريمة المعلوماتية بمعيار موضوع الجريمة وذلك كما ذهب إليه الفقيه (Rosenblatt) [4] على أنها "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغيرها أو حذفها".

والملاحظ أن التعريفات المتقدمة تضيق على نحو كبير من الجريمة المعلوماتية، حتى أن البعض يرى أن الجريمة المعلوماتية في ظل هذا الاتجاه سوف تصبح أشبه بالخرافة فحصرها مثلا في الحالات

([1]) نائلة محمد فريد قورة، المرجع السابق، ص 30.

([2]) نائلة محمد فريد قورة. المرجع السابق . ص 28.

([3]) رشيدة بوكر. المرجع السابق .ص 40.

([4]) نهلا عبد القادر المومني. الجريمة المعلوماتية. الطبعة الثانية 2010 .دار الثقافة للنشر و التوزيع ص 48.

التي تتطلب أن يكون مقترف هذه الجريمة متمتعا بقدر كبير من المعرفة التقنية لارتكابها وهو إن تحقق في بعض الأحوال فقد لا يتوفر في كثير منها، إذ قد يرتكب الفعل غير المشروع في البيئة الرقمية دون أن يكون فاعله بحاجة إلى هذا القدر من المعرفة، ورغم ذلك فإنه لا يمكن إنكار أن هذه الأفعال تدخل في عداد جرائم المعلوماتية. فالقيام مثلا بإتلاف البيانات المخزنة داخل نظام الكومبيوتر لا يتطلب من فاعله قدرًا كبيرا من العلم بتكنولوجيا الحاسبات الآلية، وعلى الرغم من ذلك فقد جرمته الكثير من التشريعات العقابية.

لذلك فانه يؤخذ على هذه التعريفات السابقة أنها جاءت قاصرة عن الإحاطة بأوجه ظاهرة الإجرام المعلوماتي، فالبعض من فقهاء هذا الإتجاه ركز على معيار موضوع الجريمة و البعض الآخر ركز على وسيلة ارتكابها و البعض الآخر ركز على معيار النتيجة .

الفرع الثاني: الإتجـــاه الموسع لمفهوم الجريمة المعلوماتية

إزاء الإنتقادات التي وجهت للإتجاه الأول حاول بعض الفقه تعريف الجريمة المعلوماتية على نحو واسع لتفادي أوجه القصور التي شابت تعريفات الإتجاه المضيق في التصدي لظاهرة الإجرام المعلوماتي.

فعلى عكسٍ من الإتجاه السابق فإن أنصار هذا الإتجاه يذهبون إلى التوسيع من مفهوم الجريمة المعلوماتية باعتبار أن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يصبغ عليه وصف الجريمة المعلوماتية. وقد تباينت مواقف أنصار هذا الإتجاه في تعريف الجريمة المعلوماتية بحسب المعايير التي اعتمد عليها كل فريق في تعريف الجريمة المعلوماتية، وتتباين مواقف الفقهاء أنصار هذا الاتجاه حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية،فيذهب فريق من الفقهاء إلى تعريفالجريمة المعلوماتية بأنها كل سلوك إجرامي يتم بمساعدة الحاسب الآلي وفريق آخر يعتبرها أنها كل جريمة تتم في محيط الحاسبات الآلية، ومن هذه التعريفات ما جاء به الفقيه (MERWE) الذي يرى أن الجريمة المعلوماتية تتمثل في الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي[(1)].

([1]) محمد أمين الشوابكة. جرائم الحاسوب و الأنترنات (الجريمة المعلوماتية) دار الثقافة للنشر و التوزيع الطبعة الأولى 2009 ص 8.

كما ذهب البعض إلى القول بأن الجريمة المعلوماتية هي كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الإتصال الخاصة به باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها.

وفي ذات الإتجاه يرى كل من Michel et credo أن الجريمة المعلوماتية تسهل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته، كما تمتد لتشمل الإعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به[(1)].

وفي هذا الاتجاه أيضا عرفها مكتب تقييم القنية بالولايات المتحدة الأمريكية بأنها الجريمة التي تلعب فيها بيانات الكومبيوتر والبرامج المعلوماتية دورا رئيسيا[(2)].

وهناك اتجاه فقهي آخر عرفها بالقول أن الجريمة المعلوماتية كل سلوك غير مشروع وغير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها[(3)].

كما عرفها الفقيهين(Richardtotty) و (Anthony Hardcastle)على أنها الجرائم التي يكون للحاسب فيها دورا إيجابيا أكثر منه سلبيا[(4)].

ولاشك أن الاتجاه المتقدم ينطوي على توسيع كبير لمفهوم الجريمة المعلوماتية، إذ يؤخذ عليه هذا التوسع الذي من شأنه أن يصبغ وصف الجريمة المعلوماتية على أفعال قد لا تكون كذلك لمجرد مشاركة الحاسب الآلي في النشاط الإجرامي، ولا يمكن القبول بهذا التوجه فقد لا يعدو أن يكون الحاسب الآلي محلا تقليديا في بعض الجرائم كسرقة الحاسب ذاته أو الأقراص أو

(1) هلالي عبد الإله أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية (دراسة مقارنة) الطبعة الأولى، دار النهضة العربية، 2000، ص 14.

(2)خالد عباد الحلبي. إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنات الطبعة الأولى، دار الثقافة 2001، ص 30.

(3) وضع هذا التعريف من طرف مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في اجتماعها المنعقد في باريس عام 1983 ضمن حلقة الإجرام المرتبط بتقنية المعلومات.

(4) محمد سامي الشوا، ثورة المعلومت وانعكاساتها على قانون العقوبات. دار النهضة العربية 1994، ص6.

الأسطوانات المغنطة مثلا، فلا يمكن إعطاء وصف الجريمة المعلوماتية على سلوك الفاعل لمجرد أن الحاسب أو إحدى مكوناته المادية كانت محلا لفعل الاختلاس[1].

ولم يسلم هذا الاتجاه من سهام النقد أيضا حين وسع من نطاق هذه الجريمة إلى درجة التسوية بين السلوك غير المشروع قانونا والسلوك الذي يستحق اللوم أخلاقيا واستهجان الكافة له، كما في التعريف الذي أورده خبراء منظمة التعاون الاقتصادي والتنمية OECD، ذلك أنه ليس بالضرورة أن يكون الإنحراف عن الأخلاق والسلوك المؤثم معاقب عليه قانونا[2].

المطلب الثالث: الطبيعة القانونية الخاصة للجريمة المعلوماتية

تعد الجرائم المعلوماتية إفرازًا ونتاجا لتقنية المعلومات،[3] فهي ترتبط وتقوم عليها. وهذا ما أكسبها لونا وطابعا قانونيا خاصا يميزها عن غيرها من الجرائم التقليدية.

والسياسية الجنائية الحديثة تستدعي منا محاولة حصر الخصائص المميزة للجرائم المعلوماتية عن غيرها من الجرائم، وذلك من أجل محاولة وضع النصوصالملائمة لمكافحة هذا النوع من الجرائم المستحدثة والتي رافقت التطور التقني والمعرفي الذي يمر به عالمنا.

فإذا كانت الجريمة بصفة عامة محل تطبيق القانون الجنائي، فإنه وبالنظر إلى الطبيعة المتميزة للجريمة المعلوماتية فإنها تتعلق غالبا بما يسمى بالقانون الجنائي المعلوماتي.[4]

وقد أضفت هذه الحقيقة على هذا النوع من الجرائم طبيعة قانونية خاصة، سواء تعلقت بذاتية هذه الجريمة أو تعلقت بخصوصية المحل الذي يقع عليه الإعتداء في ارتكاب هذه الجرائم.

([1]) نائلة محمد فريد قورة، المرجع السابق. ص 31.

([2])عادل يوسف عبد النبي الشكري. الجريمة المعلوماتية وأزمة الشرعية، دراسات الكوفة العدد السابع، ص 112.

([3]) شمس الدين ابراهيم أحمد، وسائل مواجهة الإعتدات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري-دراسة مقارنة- دار النهضة العربية الطبعة الاولى القاهرة 2005 ص 100.

([4]) أنظر في هذا المعنى محمد علي العريان –الجرائم المعلوماتية- دار الجامعة الجديدة للنشر. ص 47.

الفرع الأول: خصائص الجرائم المعلوماتية

إن ما نقصد به من ذاتية الجرائم المعلوماتية هو استقلاليتها وتميزها عن غيرها من الجرائم سيما التقليدية منها، وذلك بمجموعة من الخصائص أثرت بشكل مباشر على التشريعات العقابية والإجرائية التقليدية القائمة، وسوف نحاول أن نبرز أهم هذه الخصائص فيما يلي:

أولا: الجريمة المعلوماتية متعدية للحدود (عابرة للوطنية): إنه وبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال أسفر هذا الأمر إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة المعلوماتية الواحدة في آن واحد، حيث يمكن أن ترتكب الجريمة من مجرم في دولة على مجني عليه في دولة أخرى في وقت يسير جدًا.

فالجريمة المعلوماتية بهذا الشكل لا تعترف بالحدود بين الدول وهي بذلك شكل جديد من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة،(1) ذلك أن قدرة تقنية المعلومات على إختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث،(2) أو القيام بإعداد أحد البرامج الخبيثة (Vérus) في بلد ما ثم يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم.(3) وتظهر

(1) خالد ممدوح ابراهيم. الجرائم المعلوماتية، ، دار الفكر الجامعي، الطبعة الأولى 2009.ص 88.

(2)ائلةمحمد فريد قورة، المرجع السابق ص 52

(3) ومن الأمثلة عن القضايا التي لفتت النظر إلى البعد الدولي للجرائم المعلوماتية قضية عرفت باسم مرض نقص المناعة المكتسبة (الايدز). وتتلخص وقائعها أنه في عام 1989 قام أحد الأشخاص بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة. إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (Vérus) يترتب على مجرد تشغيله تعطيل جهاز

هذه المشكلة بصفة خاصة في التعاملات البنكية عبر شبكات المعلومات الدولية، حيث أدى التوسع الكبير لإجراء التعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بعد دولي لهذه الجرائم ذلك أن ربط وسائل الإتصالات بالحاسبات الآلية ضاعف من المعاملات المالية الدولية والتي أصبحت تتم بواسطة وسائل إلكترونية، وبصفة خاصة من خلال التحويل الإلكتروني للأموال والتبادل الإلكتروني للمعلومات.

ومفاد ما سبق ذكره أن الجرائم المعلوماتية تتميز بالتباعد الجغرافي بين الفاعل والمجني عليه ومن الوجهة التقنية التباعد بين أداة الجريمة ومحلها، وهذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة أوخارجها ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعلومات محل الإعتداء.

ولقد أثارت هذه الخاصية الدولية للجريمة المعلوماتية عدة إشكالات قانونية تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي[1] في محاكمة مرتكب هذه الجريمة، فهل هي الدولة التي وقع فيها النشاط الإجرامي أم التي أضيرت مصالحها نتيجة هذا التلاعب، بالإضافة إلى إشكالية مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة مسألة جمع الأدلة وقبولها، إذ تتباين مواقف الدول فيما يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية. وغيرها من المشاكل التي يمكن أن تثيرها الجرائم العابرة للوطنية بشكل عام.

الحاسب الآلي عن العمل ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل من خلالها بطلب مبلغ مالي يرسل على عنوان إلكتروني ليتمكن المجني عليه من الحصول على مضاد للفيروس (Antvérus) وقد تم التمكن في 1990/02/03 من إلقاء القبض على جوزيف بوب في الولايات المتحدة الأمريكية بولاية أوهايو وتقدمت المملكة المتحدة البريطانية بطلب تسليمه للمحاكمة أمام القضاء الانجليزي ذلك ان إرسال هذا البرنامج تم من داخل المملكة المتحدة وبالفعل وافق القضاء الامريكي على تسليم المتهم ووجهت له احدى عشر تهمة وقعت معظمها في دول مختلفة. وكانت لهذه القضية أهميتها من حيث أنه لأول مرة يتم فيها تسليم متهم في جريمة معلوماتية وأنها المرة الأولى أيضا التي يقدم فيها شخص للمحاكمة بتهمة إعداد برامج خبيثة (Vérus).مشار إلى هذه القضية لدى نهلا عبد القادر المومني،مرجع سابق، ص 51.

(1) تجدر الإشارة في هذا المجال إلى قضية (R.V Thompso) والتي تتلخص وقائعها في قيام مبرمج إنجليزي يعمل بأحد البنوك في دولة الكويت بالتلاعب بنظام الحاسب الآلي الخاص بالبنك ليقوم بإجراء خصومات من أرصدة العملاء ثم يقوم بإيداعها في الحساب الخاص به وبعد أن رجع المتهم إلى انجلترا قام بالكتابة إلى البنك طالبا منه أن يقوم بتحويل الحساب الخاص به إلى عدة حسابات بنكية في إنجلترا وهو ما قام به البنك فعلا. وقدم للمحاكمة أمام القضاء الامجليزي إلا أنه طعن في الحكم استنادا إلى عدم اختصاص القضاء الانجليزي بما أن فعلي السحب والايداع كانا في الكويت وليس بانجلترا.مشار إلى هذه القضية لدى نائلة عادل محمد فريد قورة ، مرجع سابق، ص 54.

لذلك فقد لفتت هذه المشكلات النظر إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجريمة المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم لمختلف الدول.

ومن أجل ذلك فقد تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لها بحزم،[1] وأن يشمل هذا التعاون تبادل المعلومات وتسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى. ولكن ومع ضرورة هذا التعاون والمناداة به إلا أنه تقف أمام هذا المبدأ عقبات ومعوقات تحول دون تحققه وتجعله صعب المنال، من أهمها انعدام نموذج موحد للنشاط الإجرامي المكون للجريمة المعلوماتية، وأن كثيرا من القوانين لم يتم تعديلها بحيث تتواءم مع هذه الجرائم حتى يتسنى إدراجها ضمن الإتفاقيات الدولية الخاصة بتبادل المساعدة الجنائية في مجال الجرائم المعلوماتية، بالإضافة إلى تنوع واختلاف النظم القانونية والإجرائية.

ثانيا: صعوبة اكتشاف الجريمة المعلوماتية وإثباتها: تقع الجريمة المعلوماتية في بيئة افتراضية تقنية لا تترك أية آثار محسوسة، إذ يغلب عليها أنها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق تلاعبهم بالبيانات، والذي يتحقق أحيانا إن لم نقل في الغالب في غفلة من المجني عليهم. كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعقد أمر كشف الجريمة وإثباتها، وإذا ما قورنت حالات اكتشاف الجريمة المعلوماتية على ضوء ما يتم اكتشافه من الجرائم التقليدية فإن عددها قليل، فمعظم الجرائم المعلوماتية تم اكتشافها بالمصادفة وبعد وقت طويل من ارتكابه، ذلك أن هذا النمط الإجرامي لا يحتاج إلى عنف أو جثث أو اقتحام وإنما هي معلومات وبيانات تغير أو تعدل أو تمحى كليا أو جزئيا من السجلات المخزونة في ذاكرة الحاسب الآلي[2] فلا تترك أثرا خارجيا مرئيا أو ملموسا فهي كما وصفها بعض الفقهاء بأنها جريمة هادئة بطبيعتها لا تتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح حتى تؤدي إلى اختراق المعلومات المخزنة في الحاسب الآلي وهتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها.[3] فالجريمة المعلوماتية من الجرائم المستحدثة التي لا تترك شهودا يمكن

---

(1) انظر في هذا المجال مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاقبة المجرمين المنعقد في هافانا عام 1990.

(2) عادل يوسف عبد النبي الشكري- الجريمة المعلوماتية وأزمة الشرعية الإجرائية- جامعة الكوفة كلية القانون، ص 116.

(3) محمد حماد مرهج البهيتي، التكنولوجيا الحديثة والقانون الجنائي. دار الثقافة للنشر والتوزيع عمان 2004، ص 165.

الإستدلال بأقوالهم ولا أدلة مادية يمكن فحصها وإنما تقع في بيئة إلكترونية يتم فيهانقل المعلومات وتداولها بواسطة نبضات إلكترونية غير مرئية.

كما ذهب البعض للقول بأن صعوبة اكتشاف الجريمة المعلوماتية وكذا صعوبة إثباتها راجع أيضا إلى عدة أسباب، من بينها وسيلة تنفيذها والتي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، إذ أنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات وذلك سواء لارتكابها أو التحقيق فيها أو لملاحقة مرتكبيها. فأحيانا نجد رجال الضبطية القضائية غير قادرين على التعامل بالوسائل الإستدلاليةوالإجراءات التقليدية مع هذا النوع من الجرائم. بالإضافة إلى صعوبة الإحتفاظ الفني بدليل الجريمة المعلوماتية، إذ للمجرم المعلوماتي القدرة على تدمير الدليل في أقل من ثانية[1].

ويمكن اعتبار أنه من بين الأسباب أيضا التي تقف وراء صعوبة اكتشاف الجريمة المعلوماتية وإثباتها المجني عليهم أنفسُهم, ذلك أن هؤلاء قد يلعبون دورا رئيسيا في ذلك من خلال الإحجام عن الإبلاغ عنها في حالة اكتشافها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للإنتهاك أو تمنى بخسائر فادحة من جراء ذلك عن عدم الكشف حتى بين موظفيها عما تعرضت له وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهزا للثقة في كفاءتها.[2] ويبدو ذلك أكثر وضوحا في المؤسسات المالية مثل البنوك والمؤسسات الإدخارية ومؤسسات الإقراض .حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضاؤل الثقة فيها من جانب المتعاملين معها، حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه، وهو ما يؤثر سلبا على السياسة التي يمكن أن توضع لمكافحتها.[3].

(1) هشام محمد فريد رستم الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة الطبعة الأولى 1994، ص 16.

(2)أشارت بعض التقديرات في الو.م.أ أن ما يتراوح بين 20 و25% من جرائم الحاسبات لا يتم الإبلاغ عنها خشية الإساءة إلى السمعة وفي دراسة أجريت على ألف شركة من الشركات المنتجة لجهاز (Fortune 500) أظهرت نتائجها أن 2% فقط من كل جرائم المعلوماتية التي يتم التبليغ عنها للشرطة أو لمكتب التحقيقات الفدرالي. مشار إليه لدى رشيدة بوكر، مرجع سابق،ص472.

(3) نهلا عبد القادر المومني، المرجع السابق، ص 55.

وقد تم طرح عدة اقتراحات تكفل تعاون المجني عليه في كشف هذه الجرائم وبالتالي إنقاص حجم الإجرام المعلوماتي الخفي، ومن هذه الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بجرائم المعلوماتية على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال مع تقرير جزاء على الإخلال بهذا الإلتزام.وعرض ذات الإقتراح على لجنة خبراء مجلس أوروبا ولاقت الفكرة رفضا باعتبار أنه ليس مقبولا تحويل المجني عليه إلى مرتكب الجريمة.

الفرع الثاني: محـــل الجريمـــة المعلوماتية

إن من جملة الإنعكاسات السلبية والخطيرة جراء سوء استخدام تقنية المعلومات والإنحراف عن الأغراض المتوخات منها، تفشي طائفة من الجرائم المستحدثة والتي كما سبق ذكره أطلق عليها عدة تسميات واستعمل في الدلالة عنها مختلف المصطلحات. وعلى العموم فقد صنفت هذه الجرائم إلى طائفتين، طائفة كانت فيها تقنية المعلومات وسيلة لارتكاب الجريمة وطائفة كانت تقنية المعلومات محلا لها.

ومن المحتم علمه أن مفهوم جرائم تقنية المعلومات قد نشأ وتطور ولا يزال يتطور تبعا لتطور التقنية واستخداماتها، وأن وجود هذه التقنية المعلوماتية في جريمة ما ليس دليلا على طبيعتها التقنية، فهناك الكثير من الجرائم التي يكون محلها النظام المعلوماتي ومع ذلك فإنها تستبعد من طائفة الجرائم المعلوماتية، ذلك أنه بالنظر إلى النظام المعلوماتي في ذاته لوجدناه ليس من طبيعة واحدة. فهو يتكون[1] من عناصر مادية وأخرى غير مادية بما يسمح من إمكانية أن يكون محلا ذو طبيعتين

([1]) نعني بنظام الحاسب الآلي كل مكوناته المادية والمعنوية. ويشمل النظام المعلوماتي على عنصرين أساسيين:

-المكونات المادية: (Hardware) و تشتمل على مختلف أنواع المكونات والوسائط المادية المستخدمة في العمليات التي تمر بها البيانات والمعلومات كوحدات الادخالin put والإخراج out put ووحدة التشغيل المركزية.و المكونات المادية لا تشتمل على الحواسيب وبقية الأجهزة بل أيضا كل الوسائط (Media) والأشياء المادية التي تسجل عليها البيانات ومن أهم مكونات النظام المعلوماتي المادية الكمبيوتر والمكونات الرئيسية واستخدامات النظام والتخزين الخارجي والاجهزة الملحقة. والمكونات الرئيسية لأي نظام معلوماتي تنقسم إلى ثلاث أجزاء رئيسية هي: وحدات الإدخال (in put) والجزء الثاني وحدة التشغيل المركزية ومن أهم مكوناتها الذاكرة وحدة الحسابات والمنطق ووحدة التحكم والجزء الثالث وحدات الإخراج (out put units)

مختلفتين أحدهما يتمثل في الجانب المادي والآخر غير المادي مما أدى إلى الإخفاق في تحديد المفهوم الدقيق لمحل الجريمة المعلوماتية، وهو الأمر الذي يطرح التساؤل عن ما هو بالضبط محل الجريمة العلوماتية ثم ماهي الطبيعة القانونية له.

أولا: تحديد محل الجريمة المعلوماتية: إنه بالنظر إلى الأهمية التي ينبغي أن يوصف بها الدور الذي يؤديه نظام الحاسب الآلي لإتمام النشاط الإجرامي في الجرائم المعلوماتية، فإن ذلك يؤدي إلى اختلاف محل الجريمة بحسب الزاوية التي ينظر إليها والدور الذي يلعبه هذا الحاسب ذاته. والذي لا يعدوأن يقوم بأحد الأدوار التالية: دور الضحية في الجريمة، دور المحيط أو البيئة التي ترتكب فيها الجريمة أو دور الوسيلة التي ترتكب بواسطتها الجريمة،[1] وعلى هذا الأساس فقد يكون الحاسب الآلي نفسه أو المعلومات المخزنة فيه محلا للجريمة وقد يستخدم الحاسب ذاته كأداة لارتكاب الجريمة. وبالتالي نفرق هنا بين ثلاث حالات:

الحالة الأولى: وقوع الجريمة على المكونات المادية للنظام المعلوماتي:إن الإعتداء على المكونات المادية للنظام المعلوماتي يتحقق إذا كان الحاسوب والأجهزة الملحقة به من معدات، وكابلات، وشبكات الربط وآلات طباعة محلا للاعتداء، وتقوم الجريمة في هذه الحالة بإتيان أي فعل مادي من شأنه إخراج الحاسوب من حيازة مالكة وإدخاله في حيازة شخص آخر، أو إتلاف الجهاز وتدميره وغير ذلك من الأفعال المجرمة.

وهذه الجرائم هي جرائم تقليدية باعتبار أن هذه المكونات المادية محل الاعتداء تتمتع بالحماية الجزائية وفق النصوص التقليدية، باعتبارها من الأموال المادية المنقولة والتي تخضع سرقتها أو إتلافها للنصوص الجزائية التقليدية القائمة ويسأل مرتكبوها بموجب النصوص العقابية القائمة في قانون

- المكونات المعنوية (المنطقية) (Software): وهي مجموعة التعليمات يمكن للنظام استخدامها بشكل مباشر وغير مباشر للوصول إلى نتيجة معينة وتنقسم هذه المكونات إلى نوعين برامج النظام أو الكيانات المنطقية الأساسية والثاني الكيانات المنطقية التطبيقية وتتمثل على كافة أنواع التوجيهات والتعليمات المطلوبة في معالجة البيانات ويلزم لهذه المكونات مصطلح آخر يسمى شبكة اتصال (Net Works) وهي سلكية ولا سلكية تقوم بعملية الربط بين الأجهزة والأنظمة المختلفة وهناك عنصر ثالث مكمل لهذين العنصرين يتمثل في العنصر البشري والذي يمكن تسميته Humanware وهو الذي يقوم بتشغيل مكونات النظام .في هذا الاطار أنظر د. أحمد خليفة الملط المرجع السابق.ص 28.

(1) مفتاح بوبكر المطردي ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقدة في 23-2012/09/25 ص 12.

العقوبات، وعلى هذا الأساس فإن المكونات المادية للنظام المعلوماتي تخرج من نطاق المحل الذي ينصب عليه السلوك الإجرامي في الجرائم المعلوماتية.

الحالة الثانية: وقوع الجريمة باستعمال أنظمة الحاسب الآلي: في هذه الحالة لا يكون الحاسب الآلي محلا أو موضوعا للجريمة وإنما يستخدم الجاني الحاسب في ارتكاب الجرائم، فما هو إذن إلا وسيلة لارتكابها، ومحل هذه الجرائم يختلف بحسب الشيء الذي ينصب عليه سلوك الفاعل والذي يشكل محلا للحق أو المصلحة المحمية.وفي هذه الحالة نكون بصدد جرائم تقليدية بحتة وإنما استعملت في ارتكابها التقنية المعلوماتية فهي بذلك ليست بحاجة لنصوص غير نصوص قانون العقوبات التقليدية لتنطبق عليها.

الحالة الثالثة: وقوع الجريمة على المكونات المعنوية للنظام المعلوماتي: وتتحقق هذه الحالة عندما تكون مكونات الحاسب غير المادية المتمثلة في المعلومات بكل صورها من البيانات والبرامج المخزنة في ذاكرة الحاسب محلا للإعتداء، كأن يتم سرقتها أو إتلافها أو تزويرها والعبث بها وغير ذلك من الأفعال غير المشروعة. وهي الحالة التي تقف النصوص العقابية التقليدية قاصرة على تحقيق الحماية الكافية والمتكاملة للمعلومات.

وترتيباً عليه فإنه يبقى في النهاية أن تكون المعلومة بمفهومها الواسع[1] هي وحدها محلا للجريمة المعلوماتية محل الدراسة، ومن ثم فقد اعتُبرت الجريمة المعلوماتية من طائفة الجرائم التي تنصب على المعلومات بكل أنواعها، سواء المدخلة أو المعالجة أو المخزنة داخل الجهاز وتستهدف هذه الجرائم الحق في المعلومات ويمتد تعبير الحق في المعلومات ليشمل الحق في انسيابها وتدفقها[2].

وحتى نجزم بخضوع فعل الإعتداء على المعلومات لنصوص قانون العقوبات التقليدي أم أنها تتطلب معالجة قانونية ذات طبيعة خاصة لابد من معرفة أولا الطبيعة القانونية للمعلومات.

(1) وتشمل المعلومات بمفهومها الواسع البيانات والمكونات المنطقية كالبرامج التطبيقية وبرامج التشغيل.

(2) خالد ممدوح ابراهيم ، المرجع السابق ص 92.

ثانيا: الطبيعة القانونية لمحل الجريمة المعلوماتية: لقد أصبحت المعلومات مصدر قوة ومصدر سلطة حتى قيل أن المعرفة هي سلطة وأن الحصول على المعرفة وحسن استخدامها عاملان أساسيان من عوامل التقدم، ولذلك فإن التكنولوجيا الحديثة تتعلق بالمعرفة ثم السلطة[1].

ونظرا لما تشغله المعلومات من قيمة اقتصادية كبيرة كان هناك تهافت من قبل الأفراد والمؤسسات المختلفة وكذا الدول للحصول عليها من أجل تسريع عملية التقدم في كل المجالات،[2] مما أدى إلى أن أصبحت المعلومات تتمتع بقيمة اقتصادية عالية قد تفوق قيمة الأموال المادية، وأصبحت المعلومات بأشكالها المتباينة في البيئة الرقمية الهدف الرئيسي لمرتكبي الجرائم المعلوماتية.

إلا أن طبيعة المعلومات في حالتها المجردة من الوسائط المادية تثير عدة مشاكل في تحديد طبيعة محل الجريمة باعتبارها مجرد إشارات أو نبضات إلكترونية غير مرئية تنساب عبر أجزاء النظام المعلوماتي وشبكات الإتصال العالمية وليست ذات كيان مادي. الأمر الذي أدى إلى خلق مواقف فقهية متباينة من أجل تحديد الطبيعة القانونية لها، أي فيما إذا كانت المعلومات تعد من القيم المالية التي يمكن الاعتداء عليها.

وقد انقسم الفقه عند الإجابة على هذا التساؤل إلى اتجاهين:

الاتجاه الأول: يرفض أنصار هذا الإتجاهاعتبار المعلومات ضمن القيم المالية التي يمكن الإعتداء عليها، ذلك أنه من خصائص القيم المالية أن تكون قابلة للتملك، ويترتب على ذلك أن الأشياء التي يمكن الإستئثار بها هي وحدها التي تدخل في عداد القيم المالية. أما المعلومات لما لها من طبيعة معنوية فإنه لا يمكن الإستئثار بها ومن ثم فلا يمكن إدراجها في مجموعة القيم المالية التي تحضى بالحماية القانونية إلا إذا تم التمكن من الإستئثار بها عن طريق حقوق الملكية الأدبية أو الفنية أو الصناعية. ولكن ونظرا للقيمة الاقتصادية للمعلومات التي لم يكن لأنصار هذا الإتجاه إنكارها، أدى بالبعض إلى إدخال المعلومات في طائفة المنافع (الخدمات Les services)، فللمعلومات في رأي أنصار هذا الإتجاه علاقة مباشرة بفكرة المنفعة أو الخدمة، ذلك أن نشأة المعلومة غالبا ما

---

(1) حسب عمرو. حماية الحريات في مواجهة نظم المعلومات، دار النهضة العربية الطبعة الأولى القاهرة 2000 ص 30.

(2) نهلا عبد القادر المومني المرجع السابق. ص 99.

تكون استنادًا إلى عمل سابق عليها، ومن جهة أخرى فإن الإلمام بالمعلومة يساعد بصفة عامة على القيام بعمل بصورة أيسر وأسرع، لذا يمكن في هذه الحالة اعتبار المعلومات كخدمة تقوم بالمال.

ومع ذلك فإن الفقه وحتى القضاء الفرنسي من أجل إيجاد حماية قانونية للمعلومات من الناحية المدنية في حال الإستلاء غير المشروع عليها حاول الإستعانة بدعوى المنافسة غير المشروعة،ثم تأسيس الخطأ على نظرية التصرفات الطفيلية ثم على نظرية الإثراء بلا سبب وأخيرا على فكرة المسؤولية التقصيرية[1].

الإتجاه الثاني: يرى أنصار هذا الإتجاه أن المعلومات تعد أموالا منقولة، وأنه يمكن تقويمها بالمال إنطلاقا من القيمة الإقتصادية لها،[2] وبالتالي تصح أن تكون محلا للحقوق المالية وعلى الأخص حق الملكية على أساس إمكانية استغلالها في تحقيق فوائد مادية ويجوز بذلك أن ترد عليها جميع أنواع التعاملات وتكون محلا للحماية القانونية المدنية والجزائية باعتبارها مالا، ويستوي في ذلك أن تكون مبتكرة أم غير مبتكرة، فإذا كانت مبتكرة فهي محمية بموجب قانون حماية الملكية الفكرية وإذا لم تكن كذلك فتكون محمية طبقا للقواعد العامة.

([1]) فقد تم اللجوء أولا إلى إدراج الخطأ الناجم عن الاستيلاء غير مشروع على المعلومات في إطار دعوى المنافسة غير مشروعة،فالخطأ في إطار هذه الدعوى يجد أساسه في الظروف المحيطة بالاستيلاء على المعلومة وليس في الاستيلاء ذاته. ولذلك من أجل تفادي الاعتراف بحق الإستئثار على المعلومة. لأن الإعتراف بالخطأ في ذاته يعني قابلية المعلومة للاستئثار بها وهو ما يرفضه أنصار هذا الإتجاه وقد استند هذا الرأي إلى المبدأ الذي أقرته محكمة النقض الفرنسية في حكمها الصادر في 1978/10/03 في شأن القضية التي تتلخص وقائعها أنه تمكنت أحد المؤسسات أثناء إجراء مفاوضات مع أحد الأشخاص من التعرف على بعض الأفكار التقنية التي توصل إليها و لم يقم بتسجيلها بعد، ولما كانت المفاوضات لم تنته بعد إلى إبرام العقد بينها فقد قامت المؤسسة بالاستعانة بهذه الأفكار في عملها. فأصدرت المحكمة ضد المؤسسة معتبرة أن الغاية من دعوى المنافسة غير مشروعة هي تأمين الحماية لكل من لا يستطيع أن ينتفع بحق استئثاري وفي حكم آخر صادر عن محكمة النقض الفرنسية أقرت المحكمة بوجود خطأ في واقعة الإستخدام غير المشروع لمعلومة تخص الغير وبدون الإحالة على دعوى المنافسة غير المشروعة والتي لم تتوافر شروطها، وتتلخص وقائع هذه القضية في تقدم إحدى المؤسسات بطلب إلى إحدى المؤسسات المتخصصة بإجراء دراسة خاصة لمخفضللسرعة يراعى فيه بعض الضوابط التقنية إلا أن المؤسسة الأولى قامت بدوها إلى تسليم البحث والتصاميم إلى مؤسسة ثالثة، وقد تعددت المحاولات من جانب الفقه لتحديد المعيار الذي اعتمدته المحكمة في حكمها السابق لتبرير الخطأ فبينما ذهب البعض إلى تبرير هذا الخطأ على أساس التطبيق الموسع لنظرية التصرفات الطفيلية.

إلا أن هذا الرأي قوبل بالرفض من البعض الآخر حيث أن وجود الخطأ استنادا إلى هذه النظرية يعني الاعتراف بحق الاستئثار على المعلومة. وهو مالا يقره جانب كبير من الفقه. وهو ما أدى البعض إلى تأسيس هذا الخطأ على نظرية الإثراء بلا سبب بوصفه تطبيق خاص لها إلا ان الحكم لم يشر إطلاقا إلى تطبيق هذه النظرية ولهذا السبب ذهب الأستاذ « Debois » إلى القول بأن الخطأ في هذه الحالة يكون على أساس المسؤولية المدنية وهو ما يراه البعض الأساس الذي ارتكز عليه الحكم المتقدم لمحكمة النقض الفرنسية حيث أسس الخطأ على فكرة المسؤولية التقصيرية.

([2])أشير إليه لدى: محمد حسام لطفي، الجرائم التي تقع على الحاسبات أو بواسطتها.بحيث مقدم إلى المؤتمر السادس للجمعية المصرية للقانون الجنائي. القاهرة خلال الفترة 25-1993/10/28.

وأن ما دفع بالفقه الحديث إلى البحث عن معيار آخر غير معيار مادية المال هو التطورات السريعة التي حدثت في مجال تكنولوجيا المعلومات والتي لا تزال مستمرة حتى الآن والتي جعلت المعلومات تنتشر بصورة كبيرة في مجال المعاملات الإلكترونية المختلفة، مما أدى في بعض الأحيان إلى ارتفاع قيمتها عن الأموال المادية، لذلك فقد تم اللجوء إلى معيار القيمة الإقتصادية للشيء حيث يعتبر الشيء مالا ليس بالنظر إلى كيانه المادي الملموس، وإنما بالنظر إلى القيم الاقتصادية له[1].

وحسب ما تقدم فإنه من الواضح أن الآراء قد تضاربت حول الطبيعة القانونية للمعلومات. فالإتجاه القديم ربط وصف المال بعنصرين هامين يكون في اجتماعهما تبلور المفهوم التقليدي للمال وهما عنصر المادية وعنصر القيمة، فإذا توافر أحدهما دون الآخر لا يتحقق في الشيء وصف المال طبقا للمفهوم التقليدي. وإن كانت النظرة التقليدية تغلب المنظور المادي على المنظور القيمي للأشياء فإن الاتجاه الحديث في الفقه يذهب إلى الأخذ بالمفهوم الموسع للمال ليشمل إلى جانب الأشياء المادية، تلك الأشياء غير المادية أخذًا في الإعتبار قيمتها الإقتصادية وهو بهذا الاتجاه يواكب القيم التي أفرزتها الثورة المعلوماتية.[2]

وهكذا نرى أن النظم القانونية القائمة التي تتناول الجرائم التقليدية التي تقع على الأموال وضعت في ظروف تختلف عن الظروف الحالية التي خلفتها ثورة تقنية المعلومات،والتي أفرزت

([1]) قال فقيه القانون المدني الفرنسي Carbonnier أن القانون الذي يرفض إسباغ صفة المال على شيء له قيمة اقتصادية قانون ينفصل تماما عن الواقع. أنظر في ذلك: السيد عتيق، جرائم الانترنت، دار النهضة العربيةالقاهرة .2000.ص 91.كما يرى السنهوري انه إذا كان التطور قد زاد من عدد الأشياء المعنوية بحيث تفوق بعضها قيمة الأشياء المادية، فإن الأمر يستدعي إعادة النظر في حصر الأموال على الأشياء المادية وحدها والبحث عن معيار آخر غير طبيعة الشيء الذي يرد عليه الحق المالي حتى يمكن إصباغ صفة المال على الشيء المعنوي انظر د. السنهوري الوسيط الجزء الثامن، ص 72

ويذهب الأستاذ Catala إلى أن المعلومات في ذاتها تعد قيمة مالية أشبه بالسلعة فهي نتاج لعمل بشري تنتمي بحسب الأصل إلى من يحوز العناصر المكونة لها بطريقة مشروعة ثم بضعها في شكل ما تكون صالحة للإطلاع عليها. وتبليغها بشكل مفهوم وبتحقق هذين الشرطين فإن المعلومات تصبح قيمة قابلة للتملك في ذاتها بغض النظر عن الوسيط المادي الذي يمكن أن يتضمنها. وقد استند هذا الفقيه إلى حجتين أساسيتين لإضفاء وصف القيمة على المعلومة بحيث يمكن تملكها. الأولى: هي القيمة الإقتصادية التي تتمتع بها المعلومة. والثانية: علاقة للتبعية التي تربط المعلومة بمؤلفها وهي العلاقة القانونية التي تربط المالك بالشيء المملوك ومن ثم كان لصاحب المعلومة الحق في ضمان سرية المعلومة وكذا الحق في طلب التعويض عن الأضرار التي تترتب على أي عمل غير مشروع يتعلق بها.

([2]) رشيدة بوكر، المرجع السابق. ص 92.

جرائم متميزة من حيث ممبناها وطبيعة محلها. فما هو موقف المشرع الجزائري من الجرائم المعلوماتية.

المطلب الرابع: موقف المشرع الجزائري من الجريمة المعلوماتية:

لم يجد المشرع الجزائري بدًا من تعديل قانون العقوبات لسد ما كان من فراغ قانوني في هذا المجال، وكان ذلك بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 المتمم والمعدل للأمر 156/66 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، ولقد جاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الإتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام، مما دفع بالكثير من الدول إلى النص على معاقبتها.وأن الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وأن هذه التعديلات من شأنها سد الفراغ القانوني.

وقد قدر المشرع في تدخله هذا أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي فتُحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة. لذلك فقد آثر المشرع الجزائري استخدامه لمصطلح المساس بنظم المعالجة الآلية للمعطيات، وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج بذلك من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابها، وحصرها فقط في صور الأفعال التي تشكل إعتداء على النظام المعلوماتي،أي الجرائم التي يكون النظام المعلوماتي محلا لها(الفرع الأول) .ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بموجب القانون رقم 04/09 المتضمن الوقاية من هذه الجرائم ومكافحتها(الفرع الثاني).

الفرع الأول: مفهوم نظـــام المعالجـــة الآلية للمعـــطيات

تبنى المشرع الجزائري للدلالة على الجريمة المعلوماتية مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرًا أن النظام المعلوماتي في حد ذاته أي المحتوى (Le contenant) وما يحتويه من

مكونات غير مادية (Le contenu)محلا للجريمة المعلوماتية، ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي يلزم تحققه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام. فإن ثبت تخلف هذا الشرط الأولي، فلا يكون هناك مجال لهذا البحث إذ أن هذا الشرط يعتبر عنصرا لازما لكل منها.

ولما كانت مكونات النظام المعلوماتي غير المادية لا تظهر على حالة واحدة إذ قد تكون مخزنة به أو منقولة منه أو عليه، فإن الأمر يتوجب التطرق لدراسة المقصود بنظامالمعالجة الآلية للمعطيات.

أولا: المقصود بنظام المعالجة الآلية للمعطيات:إن عملية معالجة المعطيات تحتاج إلى آلية منظمة تتولى عمليات جمع وتوفير المعلومات اللازمة ومعالجتها، وهو الأمر الذي ولد الحاجة إلى إجراءات ووسائل تساعد على القيام بذلك فظهر بالنتيجة مصطلح نظم المعلومات المبنية على الحاسبات الآلية، أو ما يسمى بنظام المعلومات المحوسبة، وهو نظام يعتمد على المكونات والأجهزة البرمجية للحاسوب في معالجة المعطيات واسترجاع المعلومات.

فالتطور التقني الحاصل في عالم تكنولوجيا المعلومات وما يتطلبه من ضرورة القيام بمهام توفير وجمع ومعالجة وتبادل المعلومات في نفس الوقت أدى إلى ابتكار نظام المعالجة الآلية، والذي نشأ في الحقيقة بهدف وصف الحالة التي انبثقت عن اندماج تقنية نظم المعلومات وتقنية الإتصالات عن بعد. وقد تم تعريفه على أنه عبارة عن آلية وإجراءات منظمة تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثم تحويلها إلى معلومات يسترجعها الإنسان عند الحاجة ليتمكن من إنجاز عمل أو اتخاذ قرار أو القيام بأي وظيفة عن طريق المعرفة التي يحصل عليها من المعلومات المسترجعة من النظام.

والظاهر أن المشرع الجزائري عند تعديله لقانون العقوبات وإضافته للقسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات عارضاً من خلاله صور هذه الإعتداءات لم يعرف نظام المعالجة الآلية للمعطيات، وأوكل بذلك مهمة تعريفه للفقه وقد حذا في ذلك موقف المشرع

الفرنسي عندما لم تحتفظ الجمعية الوطنية الفرنسية بالتعريف الذي تقدم به مجلس الشيوخ الفرنسي لنظام المعالجة الآلية بمناسبة تعديل قانون العقوبات(1) وحذف من النص النهائي.

وإذا كان تعريف مجلس الشيوخ الفرنسي لنظام المعالجة الآلية للمعلومات غير ملزم إلا انه يعتبر من الأعمال التحضيرية التي يمكن الإستعانة بها في تفسير غموض النص. كما يمكن للقضاء أن يستهديَ به فيما يعرض عليه من منازعات في هذا الخصوص(2).

ونرى أن المشرع حسنا فعل حينما تجنب التقيد بتعريف محدد لنظام المعالجة الآلية للمعطيات، ذلك أن العناصر التي يتكون منها هذا النظام في حالة تطور تكنولوجي مستمر يخضع للتطورات السريعة والمتلاحقة التي تطرأ على البيئة التقنية التي يمثلها والتي تتسع لإمكانية شمول وسائل تقنية جديدة، لاسيما وأن العالم الإفتراضي لا يزال في بدايته ولن يكون من السهولة احتواؤه. ومن جهة أخرى فإن نظام المعالجة الآلية للمعطيات يعد تعبيرا فنياً يصعب على المشتغل بالقانون إدراك طبيعته.

و بالرغم من ذلك فقد ذهبت بعض الدول إلى وضع تعريف للنظام المعلوماتي في قوانينها الداخلية ذات الصلة،كالقانون الأمريكي الموحد للمعاملات الالكترونية لسنة 1999، قانون مكافحة جرائم المعلوماتية السعودي الصادر بتاريخ 2007/03/26(3) قانون سلطنة عُمان رقم 2008/69 الخاص بالمعاملات الالكترونية الصادر بتاريخ 2008/05/17(4). القانون الإتحادي لدولة الإمارات رقم 02 لسنة 2006 المتعلق بمكافحة جرائم تقنية المعلومات(5). قانون مملكة البحرين رقم

(1) التعريف المقترح من مجلس الشيوخ الفرنسي اعتبر أن نظام المعالجة الآلية هو : "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط والتي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضعا للحماية الفنية"

(2) وهو ما يستفاد فعلا من أحكام القضاء الفرنسي حينما أخذ بالمفهوم الموسع للنظام حيث قضى في بعض أحكامه باعتبار شبكة الاتصال Le réseau Télecom من النظام.

(3) عرف نظام مكافحة الجرائم المعلوماتية للمملكة العربية السعودية الصادر في 2007/03/26 النظام المعلوماتي " بأنه مجموعة برامج وأدوات معدة لمعالجة البيانات وإدارتها وتشمل الحاسبات الآلية".

(4) المادة الأولى من هذا القانون عرفت النظام المعلوماتي بأنه نظام إلكتروني للتعامل مع المعلومات والبيانات بإجراء معالجة تلقائية لها لإنشاء أو إرسال أو تسليم أو تخزين أو عرض أو برمجة أو تحليل تلك المعلومات والبيانات.

(5) وعرف هذا القانون نظام المعلومات بأنه مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات أو المعلومات أو الرسائل الالكترونية أو غير ذلك.

83 لسنة 2002 الخاص بالمعاملات الإلكترونية.[1] القانون الأردني رقم 85/ لسنة 2001 الخاص بالمعاملات الإلكترونية.[2] قانون العقوبات لدولة قطر رقم11 لسنة 2004[3].

أما على المستوى الدولي فإن الإتفاقية الدولية لإجرام تقنية المعلومات وقفت عند حد هذا المفهوم عندما عرفت نظام المعالجة الآلية للمعطيات بموجب الفقرة أ من المادة الأولى من الفصل الأول بعنوان المصطلحات على "أنه كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة و التي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين بأداء معالجة آلية للبيانات.

كما أورد قانون الأونيسترال النموذجي بشأن التجارة الإلكترونية في مادته الثانية تعريفا للنظام المعلوماتي باعتباره النظام الذي يستخدم لإنشاء رسائل البيانات وإرسالها واستلامها أو تخزينها أو لتجهيزها على أي وجه آخر[4].

كما عرفته الإتفاقيةالأروبية المبرمةفي بوداسبت[5] بشأن مكافحة جرائم الفضاء المعلوماتي بأنه "كل جهاز بمفرده أو مع غيره من الأجهزة المتواصلة بينيا أو المتصلة والتي يمكن أن يقوم واحد منها أو أكثر تنفيذا لبرنامج معين بأداء المعالجة الآلية للبيانات."

كما أفردت إتفاقية المجلس الأوروبي الخاصة بحماية الأفراد من معالجة المعلومات الخاصة بهم الموقعة في 1981/01/28. في مادتها الثانية تعريفا لنظام المعالجة الآلية على أنه كل تخزين للمعلومات في الحاسوب ونقل وتبادل البرامج أو تغيير المعلومة أو مسحها.

وفي مشروع القانون العربي النموذجي الموحد لمكافحة سوء إستخدام تكنولوجيا المعلومات والإتصالات في صيغته المعدلة نجد في مادته الأولى تعريفا لنظام المعالجة الآلية للمعطيات على أنه

---

(1) عرف هذا القانون النظام المعلوماتي بأنه النظام الالكتروني لاستحداث واستخراج وتوصيل وإرسال واستقبال وتخزين أو بث أو تقديم معلومات

(2) القانون الأردني عرف النظام المعلوماتي بأنه النظام الإلكتروني المستخدم لإنشاء رسائل البيانات أو إرسالها أو تسليمها أو معالجتها أو تخزينها لتجهيزها على أي وجه آخر

(3) القانون القطري حدد المقصود بنظام المعالجة الآلية للبيانات بأنه كل مجموعة من واحدة أو أكثر من وحدات المعالجة سواء تمثلت في ذاكرة الحاسب الآلي أو برامجه أو وحدات الإدخال أو الإخراج أو الاتصال التي تساهم في تحقيق نتيجة معينة.

(4) قانون الاونيسرال كان بموجب القرار الذي اتخذته الجمعية العامة للأمم المتحدة بناء على تقرير اللجنة السادسة (A/51/628)

(5) الإتفاقية الأوروبية للجريمة الإفتراضية الموقعة في بودابست في 2001/11/23.

كل مجموعة مركبة من وحدة أو عدة وحدات للمعالجة سواء كانت متمثلة في ذاكرة الحاسوب وبرامجه أو وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة."

ومن خلال التعريفات التي تم ذكرها فإننا نستنتج أن مصطلح نظام المعالجة الآلية يستخدم في الحقل القانوني للدلالة على المعنى المقصود نفسه بهذا الاصطلاح وفقا لمفهومه العلمي، فهو إذن مصطلح ينطبق على أي نظام مهما كان مسماه يتوافر له عدة عناصر مرتبطة يبعضها بعدد معين من الروابط لتحقيق المعالجة الآلية للمعلومات من تجميعها وتخزينها ومعالجتها ونقلها وتبادلها وذلك من خلال برنامج معلوماتي.

وتبعا لذلك فإن حدود فكرة نظام المعالجة الآلية للمعطيات تقوم على أساس الروابط بين مختلف أجزاء هذا النظام والوجود المتزامن للأجهزة والبرامج.[1] فالدخول إلى برنامج من أجل تعديله أو تحويله إلى استعمال غير الإستعمال المخصص له لا يشكل جريمة معلوماتية إلا إذا كان هذا البرنامج يشارك في تطبيق فعلي داخل نظام كامل، ذلك أن البرنامج المعزول لا يأخذ تكييف النظام. وكذلك الشأن بالنسبة لأي من المكونات التي لا تشكل جزءا من النظام كما لو وقع الإعتداء على برامج معروضة للبيع، ولا يدخل أيضا في مفهوم نظام المعالجة الآلية المعلومات المخزنة والتي لا توجد بالمعالجة، أي التي تعتبر كالأرشيف فالدخول عليها لا يمثل دخولا إلى نظام المعالجة الآلية للمعطيات، ذلك أن الأموال المعلوماتية المعزولة لا تطبق عليها عموما إلا القواعد التقليدية.

ثانيا: مدى اشتراط الحماية التقنية للنظام المعلوماتي:لقد طرحالفقه القانوني مسألة هامة في شأن جرائم التعدي على نظام المعالجة الآلية للمعطيات، تتعلق بمدى اشتراط أن يكون النظام المعلوماتي متوفرا على الحماية التقنية حتى يحظى بالحماية الجزائية.

فقد ذهب الرأي الغالب في الفقه الفرنسي إلى عدم اشتراط الحماية التقنية للنظام حتى تقوم الجريمة المعلوماتية،[2] فبحسب هذا الرأي فإن نظام الأمن والحماية التقنية لا يكون سوى دور

([1]) انظر في هذا المعنى علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للنشر والتوزيع، الإسكندرية 1999، ص 21 وما بعدها.

([2]) عبد الفتاح بيومي حجازي .الجريمة في عصر العولمة دراسة في الظاهرة الإجرامية المعلوماتية. دار الفكر الجامعي. الطبعة الأولى ص 76.

إيجابي وإثبات سوء نية من قام بانتهاك النظام والدخول إليه بطريقة غير شرعية، ويدخل في عداد إثبات القصد الجنائي وهذه مسألة أخرى.[1] في حين ذهب الرأي الثاني في المسألة إلى القول بضرورة وجود نظام أمني لحماية النظام المعلوماتي حتى يعترف بتجريم الاعتداء على نظم معالجة البيانات، ويستند أنصار هذا الرأي إلى عدة حجج منها أن الاعتداء على النظام الأمني شرط مفترض لقيام الجريمة المعلوماتية، وأن القضاء يقضي بعدم العقاب على فعـــــــــل يعد اعتداء على حـــــــــق لم يتحوط لــــــــــــــــه صاحبه، بالإضافة إلى أن تغيب هذا الشرط يعد توسعا في التجريم فكل دخولٍ إذن غير مشروع يعد جريمة وهو أمر غير منطقي[2].

إلاأن هذا الشرط أصبح في الوقت الراهن بدون موضوع، ذلك أن غالبية النظم المعلوماتية تتمتع بحماية فنية على درجة عالية من الكفاءة، بل إن هناك شركات متخصصة لتقديم هذه الخدمة في ظل تقدم المعلوماتية، وأن الحماية الفنية وإن كانت هامة ولازمة فهي غير كافية للحد من الجرائم الماسة بنظم المعالجة الآلية للمعطيات فيلزم أن تكفلها حماية جزائية.

والمناقشات البرلمانية في فرنسا تؤكد أنها كانت ضد اشتراط الحماية الفنية بعد رفض وضع تعريف لنظام المعالجة الآلية للمعطيات والذي اقترحه مجلس الشيوخ الفرنسي مشيرا فيه إلى أن النظام لابد أن يكون محميا بجهاز للأمان وأن الأنظمة المحمية تقنيا هي وحدها التي تحضى بالحماية الجنائية[3].

الفرع الثاني: المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال:

إنه وقبل صدور القانون رقم 04/09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها كانت الجريمة المعلوماتية في النظام العقابي الجزائري تقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات

([1]) أحمد حسام طه تمام،الجرائم الناشئة عن استخدام الحاسب الآلي (الحماية الجنائية للحاسب الآلي)دراسة مقارنة. الطبعة الأولى .دار النهضة العربية القاهرة. ص 264.

([2]) علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي .الدار الجامعية للنشر و التوزيع . االاسكندرية.1999 ص 265.

([3]) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن .دار الجامعة الجديدة2007، ص 28.

وهي وفقا لدلالة الكلمة تنصرف إلى المعلومات و النظام الذي يحتوي عليها بما في ذلك شبكة المعلومات وهذه الأفعال في الحقيقة ما هي إلا جزء من الظاهرة الإجرامية .

لأجل هذا فقد تبنى المشرع الجزائري حديثا بموجب القانون 04/09 تعريفا موسعا للجرائم المعلوماتية واعتبر أنها تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 07 أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للإتصالات الإلكترونية وبذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للإعتداء بل توسع نطاقها لتشمل إضافة إلى ذلك تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها.

ويذهب بعض الفقه الجنائي(1)إلى القول بأن هذه الطائفة الأخيرة تشكل أهم الجرائم التي تتصل بالمعلوماتية وأكثرها إثارة للمشكلات القانونية، فهي تتكون بصفة عامة من بعض الجرائم التقليدية التي يتم ارتكابها بواسطة المعلوماتية فتكتسب داخل هذا الإطار خصائص جديدة لارتباطها بالحاسب الآلي و النظم المعلوماتية تتميز عن الصورة التقليدية لها وتؤدي بالتالي إلى صعوبة تطبيق النصوص التقليدية عليها وهي في ثوبها الجديد. ومن هذه الجرائم على سبيل المثال يمكن أن نتصور ارتكاب جرائم إرهابية ، جرائم التزوير أو جرائم أخلاقية ...بواسطة منظومة معلوماتية.

لذلك فالسؤال المطروح في هذا الصدد هو مدى قابلية وكفاية التشريعات العقابية القائمة والمنظمة للجرائم التقليدية للإنطباق على هذه الأنماط الجديدة من الجرائم.

إن الدراسة التحليلية لمختلف الإتجاهات الفقهية والقضائية أظهرت قصور نصوص التجريم التقليدية السائدة وعجزها عن الإحاطة بهذه الجرائم ومرد ذلك إلى حقيقتين قانونيتين أساسيتين:

الأولى تتعلق بمبدء الشرعية الذي يمنع المساءلة الجزائية ما لم يتوفر النص القانوني، فلا جريمة ولا عقوبة إلا بنص ومتى انتفى النص على تجريم مثل هذه الأفعال التي لا تطالها النصوص القائمة امتنعت المسؤولية وتحقق القصور في مكافحة هكذا جرائم.

---

(1) نائلة محمد فريد قورة، المرجع السابق، ص 265.

والثانية تتعلق بمسألة القياس في النصوص الجزائية الموضوعية أين يكون محضورا وغير جائز ويكاد ينحصر في الحقل الجزائي على النصوص الإجرائية كلما كانت أصلح للمتهم ومؤدى ذلك امتناع قياس أنماط الجرائم المرتكبة بواسطة منظومة معلوماتية أو عن طريق وسيلة اتصال إلكترونية على أنماط هذه الجرائم في صورتها التقليدية.

لذلك فالطبيعة الخاصة التي تتميز بها الجريمة المعلوماتية جعلتها تخلق ما يسمى بأزمة القانون الجزائي،حيث تضخم الفارق بين ما ينتج من تقنيات وبين مايرتكب بصددها من جرائم وبين ما يرصد لها من نصوص تشريعية لمواجهة هذه الظاهرة خاصة و أن القانون الجزائي لا يتطور بنفس السرعة التي تتطور بها التكنولوجيا أو مهارة الذهن البشري وتسخير هذه المبكرات للإستخدام السيء. وهو الأمر الذي لا يخلو من الحاجة إلى القوانين التي تسعى إلى استخدام تشريعات جزائية قابلة للتطبيق على هذه الطائفة من الجرائم. وهو ماسعت إلى تجسيده بعض التشريعات العقابية المقارنة نذكر منها على سبيل المثال:

- التشريع الأمريكي الذي وضع قانون آداب الإتصالات عام 1996، والذي جرم من خلاله نقل المواد الفاحشة للأطفال في أي مكان على الأنترنات،[1] بالإضافة إلى القانون الأمريكي لجرائم الكومبيوتر والأنترنات عام 1998 والذي جرم من خلاله مجموعة من الأفعال نذكر منها التحريض على الإنتحار عبر الأترنات، تحريض القصر على الأنشطة الجنسية عبر الوسائل الإلكترونية، جرائم التزوير الإلكتروني، جرائم تهديد السلامة العامة و الإرهاب الإكتروني[2].

- التشريع المغربي الذي أصدر القانون 03/03 المعدل و المتمم للقانون الجنائي المغربي[3]أين جرم في المادة 218-2منه إستعمال وسائل الإتصالات الإلكترونية في الإشادة بالأفعال الإرهابية.

أما على مستوى التشريع الجزائري فإن نص المادة 02[4]من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال غير كاف وحده لتجريم الأفعال

([1])المادة 18USC 2251 etcseqجرمت التقاط الصور الإباحية للأطفال والإعلان عنها عبر الإنترنت.

([2]) للتفصيل أكثر أنظر في هذا المعنى الأستاذ محروس نصار غايب، الجريمة المعلوماتية بحث مقدم للمعهد التقني لجامعة الأنبار منشور بتاريخ 2011/5/3. بدون ترقيم

([3]) أصبح هذا القانون يشكل الباب الأول، مكرر من الجزء الأول من الكتاب الثالث من مجموعة القانون الجنائي المغربي تحت عنوان الإرهاب.

([4]) تنص المادة الثانية من القانون 04/09 يقصد في مفهوم هذا القانون ما يأتي: "الجرائم المتصلة بتكنولوجية الإعلام والإتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام اتصالات الكترونية".

التي ترتكب بواسطة المنظومة المعلوماتية أو يسهل ارتكابها عن طريق هذه المنظومة طالما أنه لا توجد نصوص قانونية موضوعية تجرم كل فعل بعينه وتحدد أركانه والعقوبة المقررة له، وهو الأمر الذي يخالف مبدا شرعية التجريم و العقاب،[1] فعبارة "أي جريمة أخرى"التي استعملها المشرع في المادة الثانية من القانون 04/09نعتقد أنه لا يمكن القياس عليها لمتابعة أي شخص جزائيا حتى ولو ارتكب جريمة تقليدية بواسطة منظومة معلوماتية في ظل غياب النص الجزائي الذي يجرم هذا الفعل إذا ارتكب بواسطة منظومة معلوماتية صراحة.

لذلك ندعو المشرع الجزائري لتعديل النصوص القائمة لتستوعب الصور المتطورة للجرائم التقليدية والتي يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتية.[2]

(1) جاء على لسان القاضي Krever قاضي محكمة الإستئناف الكندية في معرض تسبيبه عن أحكامه ببراءة متهم في جريمة معلوماتية: إن هذا الحكم وإن كان يبدو غير مناسب للوفاء لحاجات المجتمع الحديث خاصة بعد أن دخل هذا المجتمع عصر المعلومات إلا أن الحل الوحيد في يد المشرع الذي عليه تغيير القانون لأن المحكمة ليس لها محاولة مط القوانين القديمة كي تعالج مشكلات تقع خارج تصور هذه القوانين.

(2) جرم مشروع القانون العربي النموذجي الموحد لمكافحة سوء إستخدام تكنولوجيا المعلومات والإتصال بعض الأفعال كما يلي:

- المادة السابعة:"كلمن زور المستندات المعالجة آليا.
- المادةالثامنة:"كل من استخدم المستندات المعالجة آليا مع علمه بتزويرها.
- المادة التاسعة: كل من قام بتحويل الأموال غير المشروعة أو قام بنقلها أو بتمويه المصادر غير المشروعة لها وإخفائها أو قام باستخدام الأموال أو اكتسابها ... وذلك عن طريق استخدام نظام الحاسب الآلي وشبكة المعلومات الدولية.
- المادة العاشرة: كل من تسبب عمدا في الإعتداءعلى القيم الدينية أو حرمة الحياة الخاصة أو خدش الآداب العامة وفقا للتشريع الداخلي لكل دولة باستخدام الأنظمة المعلوماتية أو الإنترنت.

المبحث الثاني:
أطـــراف الجـــريمة المعلومـــاتية

لقد أضافت المعلوماتية الكثير من الجوانب الإيجابية إلى حياتنا، إلا أنها في المقابل جلبت معها شكلا جديدًا من المجرمين اصطلح على تسميتهم بمجرمي المعلوماتية، فلم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز هذه الجريمة عن غيرها من الجرائم التقليدية فحسب، بل كان له أثره أيضا على تميز المجرم المعلوماتي عن غيره من المجرمين التقليديين.

كما ترتب على ذيوع المعارف التكنولوجية نتيجة ثورة التقنية المعلوماتية انتشار الوسائل المعلوماتية في جميع الأنشطة التي تزاول في المجتمعات الحديثة، وبالنتيجة أدى ذلك إلى توسع دائرة المتضررين من الجرائم المعلوماتية.

المطلب الأول: المجـــــرم المعـــلوماتي

إن مظاهر الخطورة التي تتجلى بها الجريمة المعلوماتية أن مرتكبيها يتسمون بالذكاء والدراية في التعامل في مجال المعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية، وإذا كان الشخص الذي يرتكب الفعل غير المشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع يعد في نظم القانون مجرما ويتعرض للعقاب، وكما هو معروف فإنه لا يمكن للعقوبة أن تحقق هدفها ما لم تضع في الإعتبار شخصية المجرم. وإذا كنا في مجال الإجرام المعلوماتي فيجب أن ننظر إلى المجرم المعلوماتي من حيث صفاته وسماته وكذا من حيث أصنافه وأنماطه.

الفرع الأول: خصـــائص المجـــرم المعلـــوماتي

يتميز المجرم المعلوماتي عن غيره من المجرمين بصفات وسمات معينة جعلت منه محل العديد من الأبحاث والدراسات، واختلف الباحثون في تحديد هذه الخصائص كما اختلفوا في مدى انطباق وصف جرائم ذوي الباقات البيضاء[1] على مجرمي المعلوماتية ذلك أن كلا من هؤلاء المجرمين قد يكون من ذوي الكفاءات، ولهم القدرة على التكيف الإجتماعي.

([1]) مصطلح المجرمين ذوي الياقات البيضاء مصطلح حديث نسبيا وأول من أطلقه هو عالم الإجتماعSutherlancأين وضح أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع وذوي المناصب الإدارية الكبيرة وتشمل أنواعا مختلفة من الجرائم كغسيل الأموال، وغير ذلك من الجرائم التي يقومون بارتكابها وهم جالسون في مكاتبهم.

ومع ذلك يمكن أن نستخلص من هذه الأبحاث[1] مجموعة من السمات التي يتميز بها المجرم المعلوماتي والتي يساعد التعرف عليها في مواجهة هذا النمط الجديد من المجرمين ومن أهم هذه الصفات:

1./ الذكــــاء: يعتبر الذكاء من أهم صفات مرتكب الجرائم المعلوماتية، لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج لذلك عادة ما يذكر أن الإجرام المعلوماتي هو إجرام الأذكياء وذلك بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف،[2] فهذا المجرم لا يمكن أن ينتميَ إلى طائفة المجرمين الأغبياء، فمن يستعين بجهاز الحاسوب للإستلاء على أسرار بنك أو شركة مخزنة به لابد أن يتميز بالمستوى الرفيع من الذكاء حتى يمكنه أن يتغلب على كثير من العقبات التي تواجهه في ارتكاب جريمته.

وتتجلى أهمية صفة الذكاء بالنسبة لمرتكب الجريمة المعلوماتية في عدم استخدامه للعنف في ارتكابه للجريمة، فالسلوك الإجرامي ينشأ من تقنيات التدمير الناعمة (Sabotage soft).

فيكفي أن يقوم المجرم المعلوماتي بالتلاعب ببيانات وبرامج الحاسب الآلي لكي يمحو أو يدمر هذه البيانات أو يعطل استخدام هذه البرامج.

2./المهـــارة: تعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم المعلوماتي والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين. ومستوى المهارة التي يكون عليها المجرم المعلوماتي هي التي تحدد الأسلوب الذي يرتكب به الجرائم، بحيث إذا كان الشخص مرتكب الجريمة المعلوماتية على قدر ضئيل من مستوى المهارة نجد أن الجرائم التي قد يرتكبها لا تتعد الإتلاف المعلوماتي أو نسخ البيانات والبرامج،[3] أما إذا كان المجرم المعلوماتي على درجة أعلى في المستوى المهاري فإن أسلوب ارتكابه للجرائم يختلف، إذ يمكنه عن طريق استخدام الشبكات

---

(1) يعد الأستاذ Parker واحدا من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتي بصفة خاصة ويرى الأستاذ Parker بداءة أن المجرم المعلوماتي، وإن كان يتميز ببعض السمات الخاصة به إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يستوجب توقيع العقاب عليه. ويرمز الأستاذ باركر لهذه الصفات بكلمة SKRAM وهي تعني المهارة (SKILLS)، المعرفة (Knowledg) الوسيلة (Resources)، السلطة (Autority) وأخيرا الباعث (Motives).

(2) غنام محمد غنام، الحماية الجنائية لبطاقات الإئتمانالممغنطة .مؤتمر الجوانب القانونية و الأمنية للعمليات الإلكترونية .دبي 2003ص 05.

(3) خالد محمود ابراهيم، الجرائم المعلوماتية. المرجع السابق. ص 135 .

بالدخول إلى أنظمة الحاسب الآلي لسرقة الأموال وارتكاب جرائم تجسس وزرع الفيروسات وغيرها من الجرائم التي تتطلب مهارة عالية في ارتكابها.

كما أن المهارة التي يتميز بها المجرم المعلوماتي تمكنه من تكوين تصور كامل لجريمته، إذ يستطيع أن يطبق جريمته على أنظمة مماثلة كتلك التي يستهدفها وذلك قبل تنفيذ جريمته، حتى لا يتفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها، فعادة ما يلجأ المجرم المعلوماتي إلى التمهيد لارتكاب جريمته بالتعرف على المحيط الذي تدور فيه، وكذا الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، ويساعده في ذلك درجة المهارة التي يتمتع بها.[1]

3./ التنظيم والتخطيط: تتميز الجريمة المعلوماتية عادة بوجود أكثر من فاعل للنشاط الإجرامي الواحد، إذ ترتكب أغلب الجرائم المعلوماتية من عدة أشخاص يحدد لكل شخص منهم دور معين، ويتم العمل بينهم وفقا لتخطيطٍ وتنظيمٍ سابق على ارتكاب الجريمة، فقد تحتاج جريمة نسخ برامج الحاسب الآلي مثلا إلى من يقوم بنسخ تلك البرامج وإلى من يقوم بعملية بيعها. كما أنه من الملاحظ أن الأشخاص الذين يقومون بخلق أو تعديل البرامج لأغراض غير مشروعة ليسوا دائما المستفيدين بطريقة مباشرة من النشاط الإجرامي. فجرائم المعلوماتية تتطلب عادة شخصين على الأقل أحدهما متخصص في الحاسبات الآلية يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط ذاته أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب،[2] وأحيانا أخرى يمكن تجنيد المجرم المعلوماتي القادر على اختراق نظم المعلومات ضمن عصابات الجريمة المنظمة عن طريق شبكة الإنترنت، ويمكن من خلال هذه الشبكة تبادل أفكار ومعلومات التطرف والإرهاب، كما يمكن الإتفاق معه على ارتكاب إحدى الجرائم الأخلاقية أو التلاعب في الحسابات أو بطاقات الإئتمان... [3].

4./المجرم المعلوماتي يبـــرر إركاب جريمته: أثبتت بعض الدراسات أنه لا يوجد شعور لدى المجرم المعلوماتي بعدم أخلاقية ما يقوم به أو بمساسه بمصالح أو قيم يحرص المجتمع على حمايتها بل لا يعتبر أن ما يقوم به يدخل في عداد الجرائم، خاصة في الحالات التي يقف فيها السلوك عند حد

---

[1]نائلة محمد فريد فورة .المرجع السابق. ص 58.

[2]نائلة محمد فريد قورة المرجع السابق .ص 61.

[3] عبد الفتاح بيومي حجازي، المرجع السابق.ص 105.

قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، لذلك فإن كثيرا من العاملين في مجال المعلوماتية لا يجدون أي خطأ في استعمال الشفرات السرية الخاصة بالدخول إلى أنظمة الحاسبات الآلية بطريقة غير مشروعة، أو في نسخ البرامج بدلا من شرائها واستعمال الحاسبات الآلية للمؤسسات التابعين لها لأغراض شخصية.وما ساعد على نماء هذا الشعور هو عدم وجود احتكاك مباشر بين الجاني والمجني عليه، فالتباعد في العلاقة الثنائية هذه يسهل المرور إلى الفعل غير المشروع ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل(1).

إلا أن الشعور بعدم أخلاقية هذه الأفعال الإجرامية المعلوماتية لدى فئة من المجرمين المعلوماتيين لا ينفي وجود مجرمين يرتكبون الإجرام المعلوماتي وهم على علم ودراية وإدراك بعدم مشروعية ولا أخلاقية هذا الفعل.

الفرع الثاني:أصنـــاف المـــجرم المعلـــوماتي

إن التسارع الرهيب في مجال التقنيات الرقمية الحديثة ساهم بدوره في التطور السريع لأنماط جريمة تقنية المعلومات بصفة عامة مما أصبح عائقا أمام دراسات علم الإجرام الحديثة التي تسعى إلى وضع تصنيف ثابت لمجرمي المعلوماتية.

إلا أنه ومن خلال تلك الملامح السابق ذكرها في خصائص المجرم المعلوماتي يمكن تصنيف مرتكبي الجرائم المعلوماتية إلى مجموعة من الطوائف، ولا يعني بطبيعة الحال أن كل مجرم يندرج ضمن طائفة محددة دون غيرها، بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة. وسوف نتناولهم بشيء من التفصيل كما يلي:

1/ فئة صغار مجرمي المعلوماتية: أو كما يسميهم البعض صغار نوابغ المعلوماتية (Pranksters) وتظم هذه الطائفة الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح دون أن تكون لديهم نية إحداث أي ضرر بالمجني عليهم، وذلك عن طريق إستخدام حاسبات آلية محمولة خاصة بهم أو حاسبات آلية خاصة بمدارسهم، ومن بينهم فئة لم تبلغ بعد سن الأهلية مفتونين كثيرا بالتقنيات الرقمية. وهم غالبا ما يكونون في مرحلة المراهقة، وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة المعلوماتية، وقد أثارت هذه الفئة

(1) سامي الشوا، الغش لمعلوماتي ظاهرة إجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي. دار النهضة العربية القاهرة 1993، ص 525.

جدلا واسعا في الوسط الفقهي، ففي حين كثر الحديث عن مخاطر هذه الفئة[1] التي يمكن أن تتحول إلى فئة القراصنة عندما يصبحون على درجة عالية من الخبرة والمهارة فيتم استئجارهم واستغلالهم في أعمال ذات أهداف إجرامية، ذهب جانب من الفقه أنه من الأحسن عدم تصنيف هؤلاء ضمن دائرة الإجرام لما لديهم من ميل للمغامرة والرغبة في البحث والإستكشاف.

2/ فئة القراصنة أو المخترقون: ويمكن تصنيفهم إلى صنفين:

- **الهاكار(Les Hakers)** [2]: وهم المتطفلون الذين يتحدون أمن النظم المعلوماتية والشبكات من خلال الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية وإنما ينطلقون من هدف اكتساب الخبرة أو بدافع الفضول أو لمجرد التحدي وإثبات الذات.[3]

- **الكراكر (Les crakers):** هم أشخاص يقومون بالتسلل إلى أنظمة المعالجة الآلية للإطلاع على المعلومات المخزنة بها لإلحاق الضرر أو العبث بها أو سرقتها وذلك بهدف التحدي الإبداعي،[4] وتتميز هذه الفئة بسعة الخبرة والإدراك الواسع للمهارات التقنية، لذلك فقد أثبت الواقع العملي أن الهاكر يستعين بالكراكر إذا ما صادفه أي نوع من أنواع الحماية،وغالبا ما يكون هدف هذه الفئة هو الحصول على المال أو بغرض الشهرة.

([1]) من أشهر الجرائم التي ارتكبت في الو م أ جريمة مراهق لم يتجاوز سنة 17 عاما يدعى "دينيسموران" والذي اختار لنفسه اسم "كوليو": حيث قام كوليو بشن سلسلة من الهجمات الإلكترونية على مواقع مهمة أنشأتها الحكومة الأمريكية على شبكة الإنترنت، ومنذ نهاية 1999 وبداية 2000 استطاع كوليو أن يحول حياة المسؤولين عن هذه المواقع إلى جحيم حيث دأب على مهاجمة موقع (DARE.ORG) المسؤول عن مواجهة مخاطر الإدمان ونفذ عمليات تخريبية عليه. وكذلك قضية تلاميذ المدرسة الثانوية في ولاية مانهاتن الذين استخدموا طرفيات غرف الدرس للدخول إلى شبكة اتصالات ودمروا ملفات زبائن الشركة في هذه العملية. وأيضا نجحت مجموعة من طلبة المدارس العليا بالو م أ تتراوح أعمارهم بين 15 و25 سنة يطلقون على أنفسهم أسرة المجموعة (414) في اختراق أنظمة نحو (60) حاسبا وذلك عام 1983 ومن بينها حاسبات وبنوك معلومات مختبر في لوس أنجلس وكذلك في مركز Salan Kottering لعلاج الأورام في نيويورك ومعهد ماسا شوسيتي للتقنية وقاعدة ماك كيلان للقوات الجوية.

([2]) عرفت إتفاقيةالأمم المتحدة لمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية رقم (55/63) المؤرخة في 2000/04/12 الهاكر (المخترق) بأنه المبرمج المتفوق جدا ولكنه يستخدم جل طاقته في الاتجاه غير شرعي لمحاولة اختراق أنظمة حاسوبية بهدف إثبات قدرته أو التباهي بها وأحيانا لأهداف إجرامية.

([3]) مصطفى محمد موسى، التحقيق في الجرائم الالكترونية. مطابع الشرطة، ط1، ص 15.

([4]) في سنة 1995 تم إلقاء القبض على أكبر هاكر ويدعى "كيفين متنيك" حيث قام على مدار 20 سنة بارتكاب عدد كبير من الجرائم الالكترونية إذ كان بإمكانه الدخول إلى أي نظام معلوماتي مرتبط بأجهزة الكمبيوتر وتعلم كسر كلمة المرور بسلاسة فائقة.

3/ **فئة المحترفين:** وتعد هذه الفئة هي الأخطر من بين مجرمي التقنية بحيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي سواء لهم أو للجهات التي سخرتهم لارتكاب جرائم تقنية المعلومات، فضلا عن تحقيق أغراض سياسية أو التعبير عن موقف فكري أو فلسفي. ويلاحظ أن الأضرار التي تترتب عن هذه الأفعال تكون بالغة الضرر بعكس الفئات الأخرى. كما أن مواجهتهم تتسم بالصعوبة بما يتمتعون به من كفاءات عالية في مجال المعلوماتية ومواكبتهم للتقنية ذاتها. ويعمل المنتمون إلى هذه الطائفة في أغلب الأحوال بطريقة منظمة بحيث ينطبق على أفعالهم وصف الجريمة المنظمة أو على الأقل يشترك في تنفيذ النشاط الإجرامي أكثر من فاعل.

4/ **فئة الحاقدين:** وهم فئة لا يسعون إلى الإشادة بالتفوق العلمي مثل صغار نوابغ المعلوماتية ولا إلى تحقيق مكاسب مادية كفئة المحترفين، وإنما هدفهم هو الانتقام كأثر لتصرف صاحب العمل معهم أو تعبيرا منهم على غضبهم من هيأة معينة .

5/وأخيرا تأتي الطائفة أو الفئة التي تضم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية ألا وهي الإهمال. فلاشك أن الإهمال في مجال الحاسبات الآلية يمكن أن يترتب عليه في كثير من الأحيان نتائج خطيرة. ففي نيوزيلاندا مثلا قام اثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات و لم يتمكنوا من إبلاغ قائد الطائرة بهذا التغيير مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل 60 راكبا كانوا على متنها وتمت محاكمتهم حينها بتهمة القتل الخطأ.[1]

المطلب الثاني: أساليب ودوافع إرتكاب الجريمة المعلوماتية

إنه وعلى خلاف الجرائم التقليدية التي تتطلب بطبيعتها نوعا من المجهود العضلي الذي قد يتخذ شكل العنف والإيذاء كما هو الحال في جريمة القتل مثلا، فان الجرائم المعلوماتية تعد بطبيعتها جرائم هادئة لا تتطلب سوى عدد من اللمسات الخاطفة على أجهزة الحاسوب حتى تؤدي إلى اختراق أكبر نظم المعالجة الآلية وهتك سريتها أو محو ما تحتويه من معلومات أو تعطيل برامجها، على اعتبار أن الجريمة المعلوماتية إنما تتم في صورة أوامر تصدر إلى جهاز الحاسوب ولا

(1) نائلة محمد فريدقورة. المرجع السابق. ص 63.

يحتاج مرتكبوها إلى القدرة والدراية في التعامل مع نظم المعالجة الآلية والإلمام بالمهارات والمعارف التقنية. فالمجرم المعلوماتي يستهدف محلا ذا طبيعة متميزة ونعني بذلك المعلومات التي تحتويها هذه النظم المعلوماتية، أي تلك الإشارات أو النبضات الإلكترونية غير المرئية التي تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الإتصال العالمية. وتبعا لذلك فإنه كلما كان للمجرم المعلوماتي خبرة ومهارة عالية في مجال المعلوماتية واستخدام شبكات الحاسب الآلي كلما زادت خطورته الإجرامية وتعاظمت لديه الدوافع والأهداف في ارتكاب الجريمة المعلوماتية.

الفرع الأول: أساليب و تقنياتإرتكاب الجريمة المعلوماتية

تتشابه جرائم المعلوماتية مع الجرائم التقليدية من حيث استخدام المجرم لوسائل وأساليب غير مشروعة في سبيل ارتكابه لجريمته، ومع ذلك فإن جرائم المعلوماتية تتميز بارتكابها من طرف مجرمين يستعملون كل ما من شأنه خداع الحاسب الآلي والتحايل على أنظمته المعلوماتية، وتتنوع أساليب ارتكاب الجريمة المعلوماتية التي يستعمل من خلالها المجرمون تقنيات مختلفة لتنفيذ جرائمهم وحتى وإن أمكن حصرها في الوضع الراهن إلا انه لا يمكن التنبؤ بالوسائل الفنية والتقنية التي قد تستحدث في مجال تكنولوجيا المعلومات،[1] ولعل من أهم هذه التقنيات هي الاختراق واستعمال البرامج الخبيثة (Vérus) [2] وسوف نحاول شرح ذلك فيما يلي:

أولا: الإختراق: « Haking »: تقوم معظم جرائم المعلوماتية على تقنية الإختراق وذلك بغرض الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات، والإختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروعة[3] .

([1]) نهلا المومني المرجع السابق، ص 125.

([2]) محمد خليفة، المرجع السابق. ص 40.

([3]) طبقا لمؤتمر سام للاختراق فإن للاختراق 06 مستويات بحسب درجة الخطورة:

- المستوى الأول: يعرف بهجوم قنبلة صندوق البريد ويؤدي إلى إعاقة النظام عن تقديم الخدمة.
- المستوى الثاني: الدخول غير مرخص به لنظام المعلومات والحسابات بما يتيح قراءة الملفات أو نسخها للمخترق غير مرخص له.
- المستوى الثالث: يتمكن المخترق فيه من الدخول إلى مواقع غير مرخص له بالدخول إليها.
- المستوى الرابع: يتمكن المخترق فيه من قراءة ملفات سرية.
- المستوى الخامس: يتمكن المخترق من نقل ونسخ الملفات السرية.

ويحتاج التسلل إلى جهاز الضحية دون علمه إلى مجموعة من الأدوات والوسائل، فقد يتم الإختراق عن طريق استعمال نظم التشغيل لكونها مليئة بالثغرات من خلال البروتوكولات التي يستخدمها نظام التعامل مع شبكة الإنترنات، فيقوم المخترق بالبحث عن ضحية من خلال معرفة رقم (IP) [1] الخاص به. ويتم البحث عن هذا الرقم بمجموعة من الخطوات يقوم بها المخترق على جهازه الذي يشترط أن يكون متصلا بجهاز الضحية عبر شبكة الأنترنت وفي نفس اللحظة، لأن هذا الرقم يتغير مع كل اتصال جديد.

وقد يتم الاختراق باستخدام البرامج،[2] ويشترط في هذه الطريقة وجود برنامجين أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم لأنه يأتمر بأوامر المخترق وينفذ المهام الموكلة إليه داخل جهاز الضحية وبرنامج آخر يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد، وأخطر هذه البرامج برنامج "حصان طروادة"،[3] وتتجلى خطورته لتميزه بالقدرة على الإختراق دون إمكانية كشفه وتتبعه والقضاء عليه واحتلال هذا البرنامج مكانا داخل النظام المخترق حتى ولو قام الضحية بحذفه فلا فائدة من ذلك، كما أنه يكفي أن يعمل البرنامج هذا لمرة واحدة فقط حتى يقوم بمهامه. ويمكن إرساله للضحية عن طريق رسائل إلكترونية أو عن طريقاستخدام برامج الدردشة.

كما قد يتم اللجوء في عملية الإختراق إلى أسلوب التفتيش في مخلفات التقنية وذلك بالبحث في مخلفات الحواسيب من القمامات والمواد المتروكة على مستوى الجهاز عن أي شيء يساعد على اختراق النظام، كالبرامج المدون عليها كلمة السر أو مخرجات الكمبيوتر التي قد تتضمن معلومات

- المستوى السادس: يتمكن المخترق من إيجاد قناة مفتوحة للدخول إلى سائر أرجاء النظام والعبث بمحتوياته.

([1]) Address IP يتطلب تشغيل نظم الإتصالاتالكومبيوترية أن تكون هناك آلية من أجل عنونة الأجهزة سواء المرسلة أو المستقبلة، كما تتطلب أيضا أن تكون هناك آلية لضمان وصول أو التحقق من وصول الإتصال أو الرسالة للجهة المقصودة والتحقق من جهة الإرسال.

ويستخدم في تحقيق هذه الغاية بروتوكول الأنترنات(Internet protocol (IP

([2]) معظم برامج الإختراق تستخدم نوعين من الملفات الأول يسمى Client.exe والثاني SERVER.EXE وكلاهما يندرجان تحت اسم TROJAN حيث يعمل ملف SERVER على فتح ثغرة في الحاسب المستهدف ليمكن ملف Client من الدخول إلى الحاسب من خلال هذه الثغرة. والمقصود بالثغرة PORT كل برنامج اختراق يعتمد على رقم منفذ خاص به يمكن المخترق من إدخال عنوان الحاسب المستهدف "L'addressr IP" ويرسل ملف الاختراق إلى الحاسب المستهدف بواسطة الطرق التالية:

- رسائل البريد الالكتروني E-MAIL - برامج الدردشة (ICQ) - إنزال البرامج من الموقع غير الموثوق به.

([3]) صمم برنامج حصان طروادة في البداية لغرض حسن ومفيد وهو معرفة ما يقوم به الأبناء على جهاز الكمبيوتر في غياب الوالدين أو معرفة ما يقوم به الموظفون على جهاز الكمبيوتر في غياب المدراء إلا أنه تطور هذا البرنامج بحيث أصبح يمكن المخترق من الحصول على كلمة السر الخاصة بالدخول إلى الجهاز والتي يستخدمها صاحب الجهاز نفسه فلا يمكن لصاحب الجهاز ملاحظة وجود دخيل.

مفيدة،[1] ومن خلال الأساليب أيضا في عملية الإختراق أسلوب المحاكات وذلك عن طريق التخفي بانتحال شخصية وصلاحيات شخص مفوض ومسموح له بالدخول إلى نظم المعلوماتية عن طريق إستخدام وسائل التعريف الخاصة به، وفيها يتم إعطاء حزم عناوين (IP) شكلا معينا لتبدو وأنها صادرة من جهاز حاسوب مسموح له بالدخول إلى تلك الأجهزة.

كما يوجد أسلوب آخر للإختراق وهو انتحال شخصية الموقع، ويعتبر هذا الأسلوب حديثا نسبيا في مجال الجرائم المعلوماتية،ويقوم هذا الأسلوب على قيامالمخترق بوضع نفسه في موقع بيـــني بين البرنامج المستعرض للحاسب الخاص بأحد مستخدمي الأنترنات وبين الموقع (WEB) ومن هذا الموقع البيني يستطيع المجرم المعلوماتي من خلال جهاز حاسوبه مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه، كما له أن يقوم بسرقة هذه المعلومات أو تغييرها. وكل ما يحتاجه من يقوم بهذه العملية هو السيطرة على أحد المواقع التي تتم زيارتها بكثرة وتحويله ليعمل كموقع بيني ثم يقوم المخترق بتركيب البرنامج الخاص به هناك، وبمجرد أن يكتب مستخدم الإنترناتإسم هذا الموقع فإنه يدخل في الموقع المشبوه الذي أعده المخترق.

ثانيا: البرامج الخبيثة (Les Vérus): تعد الفيروسات بمثابة المرض المعدي الذي يصيب المعطيات فيقضي عليها أو يشوهها فتذهب في كلتا الحالتين بفائدتها، وفيروس الحاسب الآلي يشبه إلى حد كبير الفيروس الذي يصيب الإنسان لقدرته على الإنتقال من حاسب إلى آخر[2].والفيروس في مجال المعوماتيةهو برنامج مثل أي برنامج آخر موجود على جهاز الحاسب الآلي يصمم بشكل يجعل منه قادرا على التكاثر ونسخ نفسه إلى نسخ كثيرة والإنتشار من نظام لآخر عبر شبكات الإتصال والقدرة على الإختفاء داخل برنامج سليم بحيث يصعب اكتشافه، كما أنه قد يكون مصمما لتدمير برامج أخرى أو تغيير معلومات ثم يقوم بتدمير نفسه ذاتيا دون أن يترك أي أثر يدل عليه.

([1]) منير محمد الجنبيهي،ممدوح محمد الجنبيهي جرائم الانترنات والحاسب الآلي ووسائل مكافحتها. دار الفكر الجامعي الإسكندرية ص 21.

([2]) محمد خليفة، المرجع السابق. ص 50.

ويمكن أن يصاب الحاسب الآلي بالفيروس عند تشغيل الجهاز بواسطة أسطوانة مرنة مصابة وكذا عند نسخ برنامج أو تحميل ملفات أو برامج من الإنترنات، وكذلك عند تبادل البريد الإلكتروني المحتوي على الفيروسات.

وتتمتع الفيروسات بقدرة فائقة على مهاجمة أجهزة الحاسوب والشبكات المعلوماتية وتعطيل الإتصالات وتشويه البيانات وأحيانا تضلل المستخدم ببيانات خاطئة. ويستخدم الفيروس بشكل عام لتحقيق أحد الغرضين:

- الغرض الحمائي: ويكون ذلك لحماية النسخة الأصلية من خطر النسخ غير المرخص به فينشط الفيروس بمجرد النسخ ويدمر نظام الحاسوب الذي يعمل عليه ويعد ذلك بمثابة عقوبة تلحق بالناسخ.
- الغرض التخريبي: ويتم إعداد هذه الفيروسات من طرف خبراء البرامج بهدف التخريب بحد ذاته أو إلى التخريب بهدف الحصول على منافع شخصي.(1)

ومن الآثار التي يخلفها الفيروس والتي تختلف بحسب نوعه:

- البطء الشديد في الحاسب بما يجعل التعامل معه مستحيلا.
- عدم القدرة على تشغيل معظم التطبيقات وظهور رسالة خطأ كلما تمت محاولة تشغيلها.
- مسح الملفات التنفيذية وكذا حذف جميع المعطيات الموجودة داخل القرص الصلب.

أما عن أنواع الفيروسات فهي كثيرة جدا ولا يمكن حصرها، إذ أنها آخذة في التزايد بشكل متسارع وأهمها: الفيروسات المقيمة، الفيروسات النائمة، الفيروسات الاستعراضية، فيروسات الثغرات...

(1)سامي الشوا، المرجع السابق. ص 190.

الفرع الثاني:دوافــعارتكاب الجــــــريمة المعلـــوماتية

إن الباعث أو الدافع هو العامل المحرك للإرادة التي توجه السلوك الإجرامي، وغالبا ما تتجه التشريعات العقابية إلى عدم اعتبار الدافع (الباعث) عنصرا من عناصر التجريم إلا في الأحوال التي يحددها القانون صراحة، فالجريمة تقوم بتحقيق عناصرها وأركانها أياً كان الباعث من وراء ارتكابها.

والحقيقة أنه مهما كانت درجة الدقة في رسم حدود كل طائفة من الطوائف التي ينتمي إليها مجرمو المعلوماتية فإن الدوافع الرئيسية على ارتكاب الجريمة المعلوماتية تتنوع وتتباين تبعا لطبيعة ودرجة خبرته في مجال المعلوماتية، ولا تخرج بأي حال من الأحوال عن ثلاث بواعث تحرك المجرم المعلوماتي، أما الباعث الأول فتشترك فيه الجريمة المعلوماتية مع غيرها من جرائم الإعتداء على الأموالبصورها التقليدية وهو الرغبة في تحقيق الربح وكسب المال، وأما الباعثان الآخران اللذان يميزان الجريمة المعلوماتية عن غيرها من الجرائم فيتمثل الأول في الرغبة في الدخول إلى الأنظمة المعلوماتية للحاسبات الآلية والمعلومات التي تحتويها بدافع المتعة والتسلية، وكذا الرغبة في إثبات الخبرة التقنية التي يتمتع بها الفاعل أو غير ذلك من الأغراض التي لا يكون السعي فيها إلى تحقيق ربح مادي أو الإضرار بهذه الأنظمة، ويتمثل الثاني في الرغبة في الإضرار بهذه الأنظمة وفي كل الأحوال فقد ذهب الفقه القانوني إلى إرجاع مصدر هذه الدوافع إلى نوعين دوافع شخصية وأخرى خارجية.

أولا: الدوافــع الشخصية: ويمكن رد الدوافع الشخصية لدى المجرم المعلوماتي إلى دوافع مادية وأخرى ذهنية.

1/ الدوافع المادية (تحقيق الربح وكسب المال): يعد الدافع المادي من أكثر الدوافع التي تحرك الجاني لإقتراف الجريمة المعلوماتية، وذلك أن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم المعلوماتي إلى تطوير نفسه حتى يواكب كل حديث يطرأ على التقنية المعلوماتية ويقتنص الفرص ويسعى إلى الإحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثرا وراءه،[1]

---

(1) وضاح محمود الحمود ونشأت مفضي المجالي. جرائم الانترنات،دار المنار للنشر. عمان 2005، ص 30.

فيعمد الجاني رغبة منه في تحقيق الثراء والكسب المادي إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الآلية لها من خلال اكتشافه لفجواتها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه أو لحساب شركائه أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة، كما يمكن الحصول على المكاسب المادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الإختلاس من جهاز الحاسوب، ولقد أشارت في هذا الإطار مجلة (Securite informatique) وهي مجلة متخصصة في الأمن المعلوماتي أن43% من حالات الغش المعلن عنها قد تمت من أجل إختلاس أموال،و23% من أجل سرقة معلومات و19% أفعال إتلاف و 15%الإستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية(1)

وفي حقيقة الأمر أنه في حال نجاح المجرم المعلوماتي في ارتكاب جريمته المعلوماتية فإن ذلك يدر عليه أرباحا كبيرة في زمن قياسي، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية وبنوك ومؤسسات مالية ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن جرائم المعلوماتية، فقد تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات للأنظمة المعلوماتية وأن 64% لحقت بهم خسائر مادية جراء هذه الاعتداءات(2).

2/ الدوافـــــع الذهـــنية (المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات): قد تكون الدوافع لارتكاب الجريمة المعلوماتية مجرد الشغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه.

(1) نهلا عبد القادر المومني، المرجع السابق. ص 90.

(2) وضاح محمود الحمود، المرجع السابق ص 31.

وعلى صعيد آخر قد يكون إقدام المجرم المعلوماتي على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية وإنما ينطلق من دافع التحدي وإثبات المقدرة.(1)

ثانيا: الدوافع الخارجية: قد يتأثر المجرم المعلوماتي ببعض المواقف قد تكون دافعة له على اقتراف الإجرام المعلوماتي ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن أبراز أهم هذه الدوافع فيما يلي:

1/ دافع الإنتقام: يعد هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية، ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية أو الطرد من الوظيفة، فيتولد لدى المجرم المعلوماتي الرغبة في الإنتقام من رب العمل، ومثال ذلك فقد دفع الإنتقام بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بـــ 06 أشهر وقد تحقق هذا الأمر في التاريخ المحدد من طرفه. (2)

2/ دافع التعاون والتواطؤ: هذا النوع كثير التكرار في الجرائم المعلوماتية وغالبا ما يحدث من متخصص في الأنظمة المعلوماتية أين يقوم بالجانب الفني من المشروع الإجرامي وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم.(3)

---

(1) ومن أشهر القضايا التي وقعت في مثل هذه الحالة قضية كان قد تعامل معها مكتب التحقيقات الفدرالي أطلق عليها اسم مجموعة الجحيم العالمي (Global Hell) تتلخص في تمكن مجموعة من الأشخاص من اختراق مواقع البيت الأبيض والشرطة الفدرالية الأمريكية والجيش الأمريكي ووزارة الداخلية الأمريكية وقد ظهر من التحقيقات أن هذه المجموعة تهدف إلى مجرد الاختراق أكثر من التدمير أو التقاط المعلومات الحساسة. مشار إلى هذه القضية لدى رشيدة بوكر /مرجع سابق،ص95

(2) سامي الشوا. المرجع السابق. ص 52

(3) أحمد خليفة اللط، المرجع السابق. ص 90.

وإذا كانت هذه أبرز الدوافع لارتكاب أنشطة الإعتداء على نظم المعالجة الآلية، ومع ذلك فهي ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لأن السلوك الإجرامي والدوافع لارتكاب الجريمة قد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة إلى تدميرها أو على الأقل حيازتها للقيام بعملية الإبتزاز والحصول على الأموال لذلك فإن الدوافع في ارتكاب جرائم المعلوماتية قد لا يتوقف عند هذا الحد، إذ نجد في كل جريمة جديدة دوافع جديدةبل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق مآربه الخاصة(1).

المطلب الثالث: المجـــني عليه في الجريمة المعلوماتية

إن من نتائج ثورة التقنية المعلوماتية انتشار الوسائل المعلوماتية في جميع الأنشطة التي تزاول في المجتمعات الحديثة،(2)إذ أصبحت المعلوماتية من لوازم الحياة المتطورة تعتمد عليها المؤسسات الحكومية أو الخاصة في تسيير أعمالها بشكل أساسي وأصبحت نتيجة لذلك مستودعاً لأسرارها، ولما كانت الجرائم المعلوماتية تقوم أساسا نتيجة الاعتداء على المعلومات فإن ذلك أدى إلى تنوع وتعدد فئات المتضررين من الجريمة المعلوماتية من جهة وازدياد حجم الأضرار المالية التي تخلفها(3)من جهة أخرى.

الفرع الأول: الضحية في الجريمة المعلوماتية:

لقد حددالإعلان العالمي الخاصبالمبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة الذي اعتمدته الجمعية العامة للأمم المتحدة بقرارها رقم 401434 الصادر بتاريخ 85/11/29 مصطلح الضحية والذي جاء شاملا لكل من المجني عليه والمتضرر من الجريمة.

(1) رشيدة بوكر، المرجع السابق. ص 96.

(2) محمد علي العريان،الجرائم المعلوماتية. دار الجامعة الجديدة للنشر2004.ص 67.

(3) في مناسبة مناقشة مجلس النواب الأمريكي على القانون الذي يسمح بتطبيق السجن مدى الحياة لمرتكبي جرائم تقنية المعلومات الشريرة أدلى رئيس اللجنة الفرعية المسؤولة عن الجريمة في الكونغرس الأمريكي لامارسميت بتصريح للتدليل على الخسائر الاقتصادية التي تلحق الو م أ من جراء الجريمة المعلوماتية قائلا: " مالم نستطع تأمين بنيتنا التحتية الإلكترونية فإن كل ما يحتاجه المجرم الإلكتروني لتعطيل اقتصادنا. هو نقرة بسيطة على الجهاز الحاسوب والإتصال عن طريق الإنترنت".

فوفقا لهذا الإعلان المشار إليه يقصد بالضحية الأشخاص الذين أصيبوا بضرر فردي أو جماعي بما في ذلك الضرر البدني أو العقلي أو المعاناة النفسية أو الخسارة الاقتصادية أو الحرمان بدرجة كبيرة من التمتع بحقوقهم الأساسية، عن طريق أفعال أو حالات إهمال تشكل انتهاكا للقوانين الجنائية النافذة في الدول بما فيها القوانين التي تحرم الإساءة لاستعمال السلطة، كما يشمل المصطلح أيضا حسب الإقتضاء العائلة المباشرة للضحية الأصلية أو فاعليها المباشرين والأشخاص الذين أصيبوا بضرر من جراء التدخل لمساعدة الضحايا في محنتهم أو لمنع الإيذاء"

يُبنى على ذلك أن الضحية في الجريمة بصفة عامة كل شخص طبيعي أو معنوي أصيب بخسارة أو ضرر أو بعدوان نتيجة ارتكاب جريمة سواء بفعل أو بالامتناع عن فعل.أما المقصود بالضحية في الجريمة المعلوماتية هو كل شخص أصابه ضرر مادي أو معنوي نتيجة الإستخدام غير المشروع لتقنية المعلومات، وقد يكون شخصا عاما ممثلا في مؤسسات الدولة وهيآتها وقد يكون خاصا ممثلا في الأشخاص الطبيعية أو المعنوية، وبحسب ذلك فإن الضحايا في الجريمة المعلوماتية يختلفون عن الضحايا في الجرائم التقليدية من مجرد كونهم أشخاصا عادية إلى مؤسسات مالية أو عسكرية أو قطاعات حكومية كان المجرم التقليدي لا يستطيع ارتكاب أي جرائم فيها أو في مواجهتها.

فنظرا لطبيعة استخدام تقنية المعلومات في جميع المعاملات الإقتصادية والمالية الوطنية والدولية والإعتماد عليها في تسيير شؤون الحياة اليومية بالنسبة للأفراد والشؤون العامة بالنسبة للحكومات كان من شأن ذلك أن يضفي أبعادا غير مسبوقة في توسع دائرة المتضررين من الجرائم المعلوماتية وتعدد فئاتهم.

ويلاحظ أنه من الصعوبة بما كان تقدير حجم الجريمة المعلوماتية بتحديد ضحايا هذه الجريمة على وجه الدقة، وربما يرجع ذلك إلى مجموعة من العوامل منها ما يتعلق بالجريمة المعلوماتية ذاتها ومنها ما يتعلق بالضحايا أنفسهم، فأما العوامل المتعلقة بالجريمة المعلوماتية فإن أهمها هو عدم وجود تعريف يحظى بقبول عام للجريمة المعلوماتية وهو ما يقف عائقا أمام الدراسات الإحصائية التي تهدف إلى بيان حجم الجريمة المعلوماتية، ذلك أن تحديد ما يعد جريمة معلوماتية يختلف من دولة إلى أخرى بالإضافة إلى أن الطبيعة التقنية التي تتميز بها الجريمة المعلوماتية والتي يوفرها لها الحاسب الآلي

بما يتمتع به من سرعة فائقة وقدرة عالية على التخزين يجعل من اكتشافها أمرا في غاية الصعوبة فكثيرا من الجرائم المعلوماتية قد تم اكتشافها عن طريق الصدفة(1).

وأما العوامل المتعلقة بالضحايا فيتمثل أهمها في إحجام المجني عليه عن الإبلاغ على الجريمة المعلوماتية خوفا من الفضيحة، والسبب في ذلك هو أن أكثر الجرائم المعلوماتية تقع داخل المؤسسات المالية وأكثر ما يحرص عليه القائمون على هذه المؤسسات هو السمعة المالية للمؤسسة ولذلك فهم يفضلون تحمل الخسائر التي قد تلحق بهم بسبب هذه الجرائم على ألا يعرف المتعاملون معهم بأن النظم المعلوماتية في المؤسسة قد تم التلاعب بها نتيجة لقصور ما.

وعلى الرغم من عدم دقة الإحصائيات التي تتعلق بتحديد حجم الجريمة المعلوماتية إلا أنها تساعد في إعطاء مؤشر واضح عن مدى اتساعدائرة المتضررين منها وسوف نقوم بعرض أهم فئات المجني عليهم في مجال الجريمة المعلوماتية.

أولا: المؤسسات المالية والجهات الحكومية: ينجذب مرتكبوا الجرائم المعلوماتية إلى القطاعات المالية مثل البنوك والمؤسسات المالية لتنفيذ أفعالهم الإجرامية، فهي من أكثر الأماكن استهدافا نظرا لما لها من أموال، ومن أهم هذه المؤسسات المالية البورصة . وذلك أن أي تعطيل في حركة البورصة يؤثر بدرجة كبيرة على حجم التعاملات المالية ليس فقط بين الأشخاص العاديين بل قد يصل الأمر إلى التعاملات المالية بين الدول(2).

وقد تعدت حدود الجرائم المعلوماتية القطاعات المدنية إلى المساس بصورة أكبر إلى القطاعات الخاصة بالقوات المسلحة نظرا لطبيعة وأهمية المعلومات التي تحتويها تلك القطاعات وهو ما يبرزه الإهتمام المنصب على الجاسوسية العسكرية وما استتبعه من ظهور حرب من نوع جديدة وهي الحرب المعلوماتية، تعتمد آلياتها على شبكات الحاسب الآلي في نقل المعومات فتعاظم دور النظم المعلوماتية في هذا المجال نظرا لحتمية وأهمية تخزين البيانات وسرعة معالجتها وعرضها بصورة مناسبة

(1) نائلة محمد فريد قورة، المرجع السابق.ص 80.

(2) خالد ممدوح ابراهيم. المرجع السابق. ص 150.

أمام القادة لاتخاذ القرار المناسب على أساس أهمية تلك المعلومات، مما جعل الدول تبادر إلى القيام بالتجسس على الدول الأخرى للحصول منها على المعلومات التي تجعلها قادرة على مواجهتها.

ثانيا: الأشخاص الطبيعيون:لا يقتصر تصنيف ضحايا جرائم المعلوماتية على القطاعات المالية والهيئات الحكومية والمؤسسات العسكرية فقط، بل يتعدى كذلك إلى الأشخاص الطبيعيين. فكثيرا ما تعد شبكة الأنترنات المجال الخصب لارتكاب تلك الجرائم ضدهم سيما ما يتعلق بالمساس بحق الخصوصية والبيانات الشخصية للأفراد،كما تعتبر جرائم الإتلاف المعلوماتي عن طريق الفيروسات من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر بريدهم الإلكتروني والذي يعتبر من أهم البوابات التي يقفز منها القراصنة إلى أجهزة الحواسيب الخاصة بالأشخاص[(1)].

ثالثا: مقدمي الخدمات الوسيطة في نطاق شبكة الأنترنات:وهم الأشخاص الذين يساعدون على الوصول إلى شبكة الإنترنت، فقد يمكن أن يكون الأشخاص الوسطاء ما بين الزبون(العميل)، وما بين شبكة الانترنت ضحايا للجريمة المعلوماتية وهؤلاء الأشخاص هم:

1/ متعهد الوصول: وهو أي شخص طبيعي أو معنوي يقوم بدور فني لتوصيل الجمهور المستخدم إلى شبكة الإنترنت وذلك عن طريق عقود اشتراك توصيل الزبون بالمواقع التي يريدها[(2)] وهو بذلك يقوم بدور فني بحت ولا علاقة له بالمادة المعلوماتية التي تصل إلى الزبون.

2/متعهد الإيواء l'hébergeur وهو أي شخص طبيعي أو معنوي يعرض إيواء صفحات الواب على حساباته الخادمة العملاقة وذلك مقابل أجر، فهو بمثابة مؤجر لمكان على الشبكة للزبون الذي ينشر ما يريد من نصوص أو صور أو تنظيم مؤتمرات أو ينشئ روابط معلوماتية مع المواقع الأخرى.

3/متعهد الخدمات: وهو ناشر الموقع والمسؤول عن المعلومات التي تعبر على موقعه إلى الشبكة وهو بذلك صاحب السلطة الحقيقية في مراقبة المعلومات التي يتم بثها وهو في القانون

(1) استغل بعض الأشخاص الحادث الإرهابي الذي حدث في الولايات المتحدة الأمريكية في 2001/09/11 بإنشاء عدة مواقع على شبكة الأنترنات بغرض جمع التبرعات. فأدى ذلك إلى وقوع الكثير من الشعب الأمريكي ضحية نصب.

(2) مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، 2001، ص 100.

السمعي البصري الفرنسي ملزم بإخطار النيابة العامة وملزم بالإيداع القانوني، ويقوم متعهد الخدمات بأدوار عديدة فهو ممول للخدمات ومالك للحاسب الخادم فضلا عن دوره في بث المعلومات(1).

4/ناقل المعلومات: وهو العامل الفني الذي يتولى الربط بين الشبكات بناء على عقد من عقود نقل المعلومات في هيئة حزم من جهاز المستخدم إلى جهاز الحاسب الآلي الرئيسي لمتعهد الوصول ثم نقلها من الحاسب الأخير إلى الحاسبات المرتبطة لمواقع الإنترنت أو بمستخدمي الشبكة والقانون الفرنسي عرف العامل الفني بموجب المادة الأولى من القانون96 /659 الصادر سنة 1996 المتعلق بالإتصال السمعي البصري على أنه كل شخص طبيعي أو معنوي يستغلشبكة الإتصالات عن بعد والمفتوحة للجمهور ويورد إلى هذه الأجهزة خدمة الاتصالات عن بعد.

الفرع الثاني: مخـــاطر الجريمة المعلوماتية:

لقد شهد العالم في السنوات الأخيرة تطورا غير مسبوق في مجالات الإعلام والإتصال نظرا إلى توغل وانتشار وسائل التكنولوجيا والإبتكارات المستحدثة في الأنشطة المعلوماتية ودخولها في جميع نواحي الحياة وهو ما قد يترتب عليه الخطر الكبير على البنيات المختلفة جراء الإستخدام غير المشروع لهذه التقنيات. والخطر الأكبر هو أن الجرائم المعلوماتية قد تستهدف الأمن القومي بارتكاب جرائم تمس جهات حكومية وأمنية، ليس هذا فحسب بل حتى الإضرار بالاقتصاد كونه أصبح يعتمد بصورة متزايدة على تقنية المعلومات (الاقتصاد الرقمي) مما قد يؤثر (هذا الإجرام التقني) تأثيرا كبيرا على إقتصاد أي دولة يلحق بها خسائر مالية ضخمة.

أولا:بعض التقديرات لحجم الخسائر المالية الناجمة عن الجريمة المعلوماتية: تبرز المؤشرات و الدراسات ازدياد حجم الخسائر والأضرار الناجمة عن الإجرام المعلوماتي خاصة في الدول التي تعتمد بشكل كبير على نظمالتقنية المعلوماتية، الأمر الذي يشكل تحديا كبيرا في مواجهة هذه الجرائم ومكافحتها، والخسائر الإقتصادية الناجمة عن ارتكاب الجرائم المعلوماتية تزداد وتتضاعف

(1) جميل عبد الباقي الصغير، الأنترنات و القانون الجنائي. دار النهضة العربية.القاهرة 2002.ص 164.

عندما ترتبط بالجريمة المنظمة، فالمنظمات الإجرامية لديها مهارة كبيرة في اكتشاف فرص القيام بأعمال ومشاريع جديدة غير مشروعة واستغلالها.وأن المعلوماتية والنمو المتواصل للتجارة الإلكترونية وكذا توجه الكثير من الدول نحو الحكومة الإلكترونية[1] حمل معه مجالات هائلة لتحقيق أرباح غير مشروعة[2].

وهناك من الأمثلة العديدة والمختلفة ما من شأنها أن تضع أمام أعيننا حجم الأضرار المالية التي تسببها جرائم تقنية المعلومات.فالتقرير الذي نشرته الجمعية الفرنسية لأمن المعلومات عام 1991 تضمن أن الخسائر وصلت إلى 10.4 مليار فرنك فرنسي 57% منها يرجع إلى أفعال إجرامية. وفي عام 1996انتهى التقرير الصادر عن نفس الجمعية إلى أن إجمالي الخسائر الناتجة عن المعلوماتية قدر بحوالي 12.72 مليار فرنك فرنسي.

ومن جهة أخرى توصلت الإدارة العامة للشرطة القضائية باعتبارها إحدى الجهات التي يصل إلى علمها الجرائم المختلفة بما فيها الجرائم المعلوماتية إلى أن أكثر من يتعرض لهذا النمط من الإجرام المشروعات التي تتعلق بالمعلومات بنسبة 25% يليها البنوك بنسبة 21% ثم المشروعات التجارية المختلفة بنسبة 18% وأخيرا الجهات الحكومية بنسبة 17%.

أما في الولايات المتحدة الأمريكية فإن إحصائيات مكتب التحقيقات الفدرالي توضح أن متوسط الخسارة في الجريمة المعلوماتية الواحدة حوالي 500ألف دولار بينما في جريمة سرقة عادية فمتوسط الخسارة 2500 دولار، أي أن متوسط الخسارة في الجريمة المعلوماتية أعلى بـــ 150 مرة عنه في الجرائم العادية، كما أصدر المركز القومي للمعلومات الخاصة بجرائم الحاسب الآلي في الولايات المتحدة الأمريكية دراسة معتمدا فيها على المعلومات التي توصل إليها معهد ستانفورد

([1]) لما ظهرت شبكة الأنترنات بخدماتها المتعددة عمدت الدول إلى استثمارها في تنفيذ التعاملات الحكومية بشكل إلكتروني لما في ذلك من تسيير تقديم الخدمات والارتقاء بمستوى المواطن وتحقيق العبء على المؤسسات الحكومية المختلفة مما يؤدي إلى زيادة كفاءتها. وقد عرفت الأمم المتحدة الحكومة الإلكترونية على أنها استخدام الانترنات والشبكات العالمية العريضة لتقديم معلومات وخدمات الحكومة للمواطنين كما عرفتها منظمة التعاون الاقتصادي والتنمية عام 2001 على أنها استخدام تكنولوجيا المعلومات والاتصالات وخصوصا الانترنات للوصول إلى حكومات أفضل.
ويبنى على ذلك أن فكرة الحكومة الالكترونية تقوم أساسا على تجميع الأنشطة والخدمات المعلوماتية في موقع الحكومة الرسمي على شبكة الانترنات في نشاط أشبه ما يكون بفكرة مجمعات الدوائر الحكومية وتحقيق حالة إتصال دائم بالجمهور مع القدرة على تامين الاحتياجات الاستعلامية والخدمية للمواطن.

([2]) نائلة محمد فريد قورة.المرجع السابق. ص 70.

الدولي للأبحاث أسفرت عن مجموعة من النتائج أهمها أن الخسائر الناجمة عن الجريمة المعلوماتية تقدر من 03 إلى 05 مليار دولار وأن المشروعات التجارية هي الأكثر عرضة لهذه الجرائم ثم يأتي بعد ذلك البنوك والمؤسسات الحكومية[1].

كما بينت دراسة أخرى أجريت من قبل منظمةThe conputersecurityinstitute أن خسائر 163 شركة أمريكية من الجرائم المتعلقة بتقنية المعلومات قد بلغت أكثر من 125 مليون دولار، كما أظهر المسح الذي أجري عام 2000ارتفاع عدد تلك الشركات المتضررة من تلك الجرائم حيث وصل إلى 273 شركة بلغ مجموع خسائرها أكثر من 256 مليون دولار.

كما ورد في التقرير السنوي الثامن لمكتب التحقيقات الفدرالي الأمريكي الصادر عام 2003 بعنوان جرائم الحاسب بأن أكثر خسائر المؤسسات بالولايات المتحدة الأمريكية أتى من الاستيلاء على المعلومات والتي كبدها خلال هذا العام خسائر تتعدى 70 مليون دولار أمريكي ويأتي في المركز الثاني نشاط تعطيل نظم المعلومات محققا خسائر تتجاوز 65.5 مليون دولار.

ثانيا: مخاطر الجريمة المعلوماتية في الجزائر:أما في الجزائر فإن المحيط الكمي للإجرام المعلوماتي غير واضح لعدم وجود دراسات وبحوث من شأنها كشف اللثام عن أرقام ومؤشرات للخسائر في بلادنا جراء هذا النمط الإجرامي[2]. وإن كانت الجزائر ليست بمنأى عن خطورة الجرائم المعلوماتية طالما أنها تحتل جزءا من الفضاء الإلكتروني خاصة فيما يتعلق بالحوسبات المالية وبعض الهيآت الحكومية التي يعتبر اختراق مواقعها ضمن حجم الأضرار الناتجة عن الجريمة المعلوماتية.

ونخلص للقول بناءا على ما تقدم أن معدل الخسائر المالية نتيجة الجريمة المعلوماتية يفوق في كثير من الأحوال نفس المعدل في الجريمة التقليدية، ويرجع السبب في ذلك إلى الكم الكبير من المعلومات (ذات القيمة المالية العالية) التي يتم برمجتها آليا والتي يمكن التلاعب بها في ثوان معدودات وتحويلها من شخص لآخر.

([1]) نائلة محمد فريدفورة،المرجع السابق ص 84.

([2]) غياب إحصاءات لهذا النوع من القضايا راجع لعدم وعي المجتمع المحلي بمخاطرها، بالإضافة إلى حداثة الثورة التقنية بالجزائر وقصور البنية التحتية اللازمة لدخول المؤسسات الوطنية بقوة في أعمال التجارة الإلكترونية.

المطلب الرابع: الحماية الفنية للمنظومة المعلوماتية

إن المنع الجنائي وتحديد عقوبات لجرائم المعلوماتية بصفة مسبقة بما يتماشى مع مبدأ الشرعية وإن كان يوفر حماية أساسية للنظام وللمعلومات ضد المخاطر والأضرار الناجمة عن هذه الجرائم من إتلاف وتدمير باهظ التكلفة في حالة الوصول إلى معلومات سرية، إلا أنه غير كاف لوحده، فحتى تكون هناك الفعالية في الحركة والأداء لابد أن تعززها حماية فنية تعمل على الحيلولة دون وقوع هذه الجرائم أو التخفيف من آثارها إذا وقعت[1].

ويقصد بالحماية الفنية أو أمن المعلومات[2] دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها، أو استغلال نظمها في ارتكاب الجريمة باعتبارها إجراءات وقائية لتجنب اختراق النظام المعلوماتي.

ويشترط لضمان توفر الحماية الفنية الكافية للمعلومات الإلكترونية السرية أو الموثوقية التكاملية, سلامة المحتوى، استمرارية توفر المعلومات وأخيرا عدم الإنكار.فماهي الوسائل الفنية اللازمة لتأمين حماية هذه المعلومات غير العقاب الجنائي.

تتعدد وسائل الأمن التقنية المتعين استخدامها في بيئة المعالجة الآلية للمحافظة على المعلومات بشكل آمن كما تتعدد أغراضها ونطاقات استخدامها.

الفرع الأول: الحماية الفنية عن طريق البرامج:

ويمكن تصنيف هذه الوسائل في ضوء غرض الحماية إلى الوسائل التالية:

1. الوسائل المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته: وهي الوسائل التي تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بهذا الاستخدام وتضم هذه الطائفة كلمات السر بأنواعها، البطاقات الذكية المستعملة للتعريف، وسائل التعريف

---

(1) وهذا ما أكدت عليه المذكرة التفسيرية لاتفاقية بودابست حينما ذهبت إلى القول من أن الوسيلة الأكثر فعالية لمنع الولوج غير المصرح به تتمثل بطبيعة الحال في التهديد بقانون العقوبات، ومع ذلك فإن هذا العرض لا يكون مكتملا دون تبني ووضع إجراءات أمنية فعالة. أنظر في ذلك د.هلالي عبد الله أحمد. الجوانب الإجرائية و الموضوعية لجرائم المعلوماتية على ضوء اتفاقية بودابست. دار النهضة العربية .القاهرة2003 ص 71.

(2) خالد ممدوح ابراهيم، أمن المعلومات،المرجع السابق. ص 38.

البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي كما تظم أيضا ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ.

2. الوسائل المتعلقة بالتحكم في الدخول والنفاذ إلى الشبكة: وهي الوسائل التي تساعد على التأكد من أن الشبكة قد استخدمت بطريقة مشروعة ومن أهم الوسائل الفنية المعتمد عليها ما يعرف بالجدران النارية والتي هي عبارة عن برامج تثبت داخل النظام بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلىالجهاز أثناء التعامل مع شبكة الإنترنات، فيتم إجبار جميع عمليات الدخول إلى الشبكة أو الخروج منها بأن تمر من خلال هذا الجدار الناري والذي يمنع أي مخترق أو متطفل من الوصول إلى الشبكة. وذلك عن طريق مراقبة الحزم الذي يتم إرسالها واستقبالها من الحاسب الآلي الخاص بالمستخدم. وعند مراقبة الجدار الناري لهذه الحزم والمنافذ التي ترسل وتستقبل من خلالها فإن عليه السماح أو الاعتراض على دخول هذه البيانات أو خروجها. وتنبه المستخدم لذلك.

3. الوسائل التي تهدف إلى منع إفشاء المعلومات لغير المخولين أو المصرح لهم بذلك: وتهدف هذه الوسائل إلى ضمان سرية المعلومات وتشمل تقنيات تشفير المعطيات والملفات، إجراءات حماية نسخ الحفظ الاحتياطية، برامج الفلترات(Filtration) والموجهات.

4. الوسائل التي تهدف إلى حماية التكاملية وسلامة المحتوى وهي الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة لها ذلك، ومن أهمها برامج تحري الفيروسات (ومضادات الفيروسات) Antivirus.

5. الوسائل المتعلقة بمنع الإنكار: وتهدف هذه الوسائل إلى ضمان عدم قدرة الشخص المستخدم على إنكار أنه هو الذي قام بالتصرف، وترتكز هذه الوسائل بصفة أساسية على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة من طرف ثالث.

6. وسائل مراقبة الإستخدام وتتبع سجلات النفاذ والأداء وهي التقنيات التي تستخدم لمراقبة مستخدمي النظام وتحديد الشخص الذي قام بالعمل المعين في الوقت المعين وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الإستخدام.

وهذه الوسيلة قد أشار إليها المشرع الجزائري في القانون 04/09 (التزامات مزودي الخدمة) في المادة 10 منه، حينما ألزم مقدمي الخدمات العمل على حفظ المعطيات التي تسمح بالتعرف

على مستعملي الخدمة المتعلقة بتاريخ ووقت ومدة كل اتصال بالإضافة إلى حفظ المعطيات التي تسمح بالتعرف على المرسَل إليه الاتصال وعنوان الموقع المطلع عليه.

وتجدر الإشارة أن كل مؤسسة أو هيأة لها طريقتها الخاصة في توفير الأمن الفني في حدود متطلبات حماية المعلومات، فلا تكون إجراءات الأمن الفني، رخوة ضعيفة لا تكفل الحماية وبالمقابل لا تكون مبالغاً فيها إلى حد يؤثر على عنصر الأداء في النظام محل الحماية، فتعقيد الحماية على المعلومات لدرجة يصعب فيها حتى على المخولين الوصول إليها قد يدفع لاحقا إلى إهمال كل الإجراءات الأمنية، مما يجعل المعلومات عرضة للخرق وهذا ما يسمى لدى الخبراء التقنيين في مجال أمن المعلومات "التأثير على صحة الأداء وفعاليته".

وفي الحقيقة فإن جميع هذه الوسائل الغرض منها هو تحقيق أمن معلوماتي أفضل ضمن فضاء افتراضي يتم فيه تبادل المعلومات الرقمية وتجري عبره كافة أنواع المعاملات والخدمات الالكترونية بواسطة تقنيات وبرمجيات وبروتوكالات تتجدد وتتطور بشكل متسارع، لذلك فإن الأمر يقتضي إجراء عمليات تقييم للآثار الناجمة عن هذه الوسائل من أجل الوقوف على مدى نجاعتها في تحقيق النتائج المرجوة منها.

الفرع الثاني: الحماية الفنية عن طريق نظام الرقابة الوقائية عبر الوسائل الالكترونية

من القواعد الفنية الوقائية التي تسمح بالرصد المبكر للإعتداءات المحتملة على النظام والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها نظام المراقبة الإلكترونية، إذ يعد هذا النظام من بين أهم آليات الوقاية من جرائم المعلوماتية.

ويقصد بمراقبة الإتصالات الإلكترونية، العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبطا بالزمن لتحقيق غرض أمني(1).

(1) رشيدة بوكر،المرجع السابق. ص 370.

ولم يتطرق المشرع الجزائري شأنه شأن التشريعات المقارنة إلى تحديد المقصود بمراقبة الإتصالات الإلكترونية، مكتف فقط بتحديد مفهوم الإتصالات الإلكترونية(1) رغم أخذه بهذا النظام بموجب المادة 03 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، والتي تنص على إمكانية وضع الترتيبات التقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها، إذا تطلبت ذلك حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية. وذلك مع مراعاة الأحكام القانونية التي تتضمن سرية المراسلات والإتصالات.(2)

وفي هذا الإطار نجد أن المشرع الجزائري قد ميز بين نوعين من المعطيات المعلوماتية محل المراقبة الإلكترونية، وهما المعطيات المتعلقة بحركة السير (معطيات المرور) والمعطيات المتعلقة بمحتوى الإتصال، فبالنسبة للنوع الأول فقد عرفها المشرع بموجب المادة 02 من القانون 04/09 بأنها "أي معطيات متعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات توضح مصدر الإتصال، والوجهة المرسلة إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة،(3) أما النوع الثاني والمتعلقة بالمحتوى فلم يأت على تعريفها، وإن كانت تتعلق بمضمون الإتصال أو الرسالة أو المعلومات المنقولة عن طريق الإتصال فيما عدا المعطيات المتعلقة بالمرور، واعتبر المشرع أن هذا النوع الأخير من المعطيات هو ما يكون محلا للمراقبة الإلكترونية عندما أدرجها في المادة 04 تحت مسمى مراقبة الإتصالات

---

(1) المادة 02 من القانون 04/09 عرفت الاتصالات الالكترونية بأنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية".

(2) نصت المادة 21 من الإتفاقية الأوروبية لمكافحة الجريمة المعلوماتية بودابست تحت عنوان إعتراض معطيات المحتوى على أنه: "يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل تخويل السلطات المختصة فيما يتعلق بالجرائم الخطيرة التي يحددها القانون الداخلي المكنات التالية:

- جمع أو تسجيل عن طريق تطبيق الوسائل الفنية المتواجدة على أرضه.
- إلزام مقدم الخدمة في نطاق قدراته الفنية المتوافرة على أن يمنح السلطات المختصة عون ومساعدته من أجل تجميع أو تسجيل في الوقت الفعلي المعطيات المتعلقة بمحتوى إتصالات معينة.

(3) نصت المادة الأولى من اتفاقية بوادابست على تعريف لمعطيات المرور كما يلي: "أنها كل البيانات التي تعالج الإتصالات التي تمر عن طريق نظام معلوماتي والتي تتم إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال مع تعيين المعلومات التالية: أصل الإتصال مقصد الإتصال الجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ الاتصال، حجم وفترة الاتصال، أو نوع الخدمة".

الإلكترونية، أما النوع الأول فقد خصها بإجراء آخر تحت مسمى حفظ المعطيات المتعلقة بحركة السير في المادة 11.

وقد أكدت إتفاقيةبوداسبت هذا التمييز، حيث أدرجت كل إجراء على حدى تحت عنوان خاص، فخصت حركة المعطيات بعنوان التجميع في الوقت الفعلي لمعطيات المرور (المادة 20) أما محتوى المعطيات فجاء تحت عنوان إعتراض معطيات المحتوى".

والملاحظ أنه وإن كان من المقبول أن كلا من النوعين من المعطيات يمكن أن تمس مصالح ذات طبيعة خاصة، إلا أنه وبالنسبة لمعطيات المحتوى فإن المصالح الفردية تكون أعلى نظرا لطبيعة محتوى المعطيات، ومن هذا المنظور يمكن فرض قيود على محتوى المعطيات بشكل أشد من تلك الخاصة بمعطيات المرور.

ومما لاشك فيه أن هذه المراقبة الإلكترونية لمحتوى الإتصالات الإلكترونية من شأنها المساس بالحق في الخصوصية، لذلك فإنه ينبغي إحاطتها بجملة من الضمانات بغرض تحقيق التوازن بين حق الإنسان في الخصوصية وحماية سرية إتصالاتهو حق المجتمع في مقاومة الجريمة. ولعل أهمها أن يتم تنفيذ هذا الإجراء بإذن من القضاء. وأن تكون ثمة ضرورة تدعو إليه وفي نطاق ضيق من أجل الوقاية من الجرائم التي تمس حقوقا ذات أهمية لاعتبارات يقدرها المشرع. وهو ما سنأتي على بيانه في حينه.

المبحث الثالث

المواجهة التشريعية الموضوعية للجريمة المعلوماتية

إن للطبيعة الخاصة للجرائم المعلوماتية أثر على التشريعات العقابية القائمة، فالقصور الذي يعتري هذه الأخيرة في مواجهتها للجرائم المعلوماتية قد يترتب عليه آثار خطيرة تتمثل في إمكانية إفلات الجناة من العقاب بسبب عدم تقنينها في صورة جرائم ينص عليها المشرع، وما قد ينجر عليه من توسع القضاء في تفسير النصوص العقابية التقليدية فيتم العصف بمبدأ الشرعية.

وقد تباينت إتجاهات الدول المختلفة في التعامل مع ظاهرة الجريمة المعلوماتية ويرجع ذلك بصفة أساسية إلى اختلاف الأنظمة القانونية لهذه الدول من ناحية، وإلى اختلاف تجربة كل منها مع الجريمة المعلوماتية من ناحية أخرى، وإلى النتائج الاقتصادية المترتبة عن الجريمة المعلوماتية والتي تختلف من دولة إلى أخرى من ناحية ثالثة. وهو ما ينعكس على أشكال السلوكات التي تلقى اهتماما من قبل المشرعين.

وإن كانت جميع الدول تتجه إلى ضرورة التدخل التشريعي لمواجهة الجريمة المعلوماتية فإنها تختلف من حيث الأساس الذي يرتكز عليه هذا التدخل التشريعي،[1] وذلك باختلاف المفاهيم القانونية التي تؤثر في النظام القانوني بشكل عام، ويمكن التمييز في هذا الصدد بين ثلاث مواقف تشريعية يتأثر مضمون الحماية الجنائية لنظم المعلوماتية بحسب المصلحة المحمية فما حماه البعض لم يحمه البعض الآخر.

الإتجاه الأول: الهدف فيه من الجريمة المعلوماتية هو حماية الملكية الفكرية، و يرى هذا الاتجاه أن المعلومات المخزنة بالحاسب الآلي والبرامج الخاصة به لا تختلف عن الأشياء التي تكون محلا لحق الملكية، لذلك تقوم التشريعات التي تأخذ بهذا الإتجاه ببسط حمايتها على النظم المعلوماتية في إطار حماية الملكية الفكرية.

([1])د. نائلة محمد فريد قورة.المرجع السابق.، ص 306.

الإتجاه الثاني: يركز هذا الإتجاه على حماية مصلحة سلامة المعلومات مهما كانت طبيعة النشاط الإجرامي الذي تتعرض له.

الإتجاه الثالث: يهتم هذا الإتجاه بالمعلومات في حد ذاتها، فالهدف في هذا الاتجاه هو حماية سرية المعلومات، فيمنع الإطلاع عليها سواء كانت هذه المعلومات متعلقة بالأشخاص أو كانت متعلقة بأشياء لها قيمة اقتصادية، أو كل معلومة يخشى من الإطلاع عليها.

و لم يقف الإختلاف بين التشريعات في التعامل مع الجريمة المعلوماتية عند هذا الحد بل يظهر أيضا بوضوح في شكل هذا التدخل الذي قد يأخذ عدة أنماط تتمثل إما في خلق نصوص قانونية جديدة يضاف إليها البعد الخاص بالنظم المعلوماتية أو تعديل بعض النصوص القانونية القائمة بحيث تتواءم مع هذا الشكل الجديد من الجرائم.

و لم يقف الأمر عند التشريعات الداخلية في مواجهة المعلوماتية، فخطورة هذه الجريمة وطبيعتها الدولية وعجز الدول فرادى عن التصدي لها جعل منها شأنا دوليا دفع بالمجتمع الدولي إلى توحيد جهوده وحشد قواه لمكافحة هذه الجرائم، فعقد المؤتمرات وسنالإتفاقيات وهو ما سوف نعرج عليه فيما يلي:

المطلب الأول: حماية النظم المعلوماتية على مستوى التشريعات الوطنية

لقد ألقت الثورة المعلوماتية بضلالها على قوانين العقوبات لمختلف الدول بالتصدي للجانب السلبي منها مع ضرورة مراعاة تحقيق هدفين أساسيين هما: عدم تفويت الفرصة في الإستفادة من تطور التقنية المعلوماتية ومن ناحية أخرى ضرورة حماية الإقتصاد والأمن الوطني وحقوق وحريات الأفراد من جراء اللجوء إلى الاستخدام غير الشرعي لهذه التقنية.

والملاحظ في هذا الصدد أنه كلما كان الاعتماد أكبر على التقنية المعلوماتية كلما كانت الحاجة أكثر إلحاحا لوضع نصوص قانونية لحماية هذه المعلوماتية.(1) وسوف نتناول فيما يلي تجربة المشرع الجزائري ثم التشريع المقارن في مكافحة الجريمة المعلوماتية.

---

(1) محمد خليفة .المرجعالسابق.ص 61.

الفرعالأول: مواجهة التشريع الجزائري للجريمة المعلوماتية:

نتيجة لتأثر الجزائر بما أفرزته ثورة تقنية المعلومات من أشكال جديدة للجرائم طالت مصالح جديدة غير تلك التي يحميها قانون العقوبات، فقد تطرق المشرع الجزائري إلى تجريم أفعال المساس بأنظمة المعالجة الآلية للمعطيات من خلال تعديل قانون العقوبات بموجب القانون رقم 15/04والذي تضمن ثمانية موادعمد المشرع من خلالها إلى حماية سرية وسلامة المعلومات ونظم معالجتها وذلك من المواد 394 مكرر إلى 394 مكرر 07،أين جرم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو في جزء منه المادة (394 مكرر).

- الإدخال بطريق الغش معطيات في نظام المعالجة الآلية أو الإزالة بطريق الغش لمعطيات يتضمنها نظام المعالجة (394 مكرر1)
- الإتجار في معطيات مخزنة ومعالجة أو مرسلة عن طريق منظومة معلوماتية.
- حيازة أو إنشاء أو نشر المعطيات المتحصل عليها بارتكاب إحدى الجرائم المنصوص عليها في هذا المجال.

والملاحظ أن تخصيص المشرع الجزائري لهذه الجرائم قسما خاصا في قانون العقوبات دلالة على إقراره بأنها ظاهرة مستجدة ومتميزة عن الجرائم التقليدية الأخرى من حيث المصالح التي تطالها وكذا من حيث مبناها وطبيعتها ومحلها، ومن ثم لا يمكن إدراجها تحت أي نوع من الجرائم التقليدية.[(1)]

كما أنه لم يميز في وضعه لهذه النصوص القانونية نوعية المعلومات التي تطالها الجريمة فيما إذا كانت معلومات تتصل بمصالح اقتصادية أو مالية أو مسائل أمنية، وذلك سعياً من المشرع الجزائري إلى تعميم الحماية للمعلومات بكافة أنواعها ما عدى تشديد العقوبة إذا كانت المعلومات المستهدفة متعلقة بالدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

وفي الحقيقة فإنه قبل هذا القانون نجد أن المشرع الجزائري قد حاول مواجهة الجريمة المعلوماتية من خلال قانون الملكية الأدبية والفنية وهو الأمر 14/73 المؤرخ في 1973/04/03 المعدل

(1) رشيدة بوكر، المرجع السابق.ص 127.

والمتمم بمقتضى الأمر 10/97 المؤرخ في 1997/03/06 والمعدل والمتمم بالأمر 05/03 المؤرخ في 2003/07/19. والمتعلق بحق المؤلف والحقوق المجاورة، حينما أدمج بموجب هذين الأمرين الأخيرين برامج الإعلام الآلي ضمن المصنفات الأصلية التي تشملها الحماية القانونية[1] وقرر للإعتداء عليها عقوبة الحبس والغرامة.

وتجدر الإشارة إلى أن هذه المستجدات التي اعتمدها المشرع الجزائري من خلال الأمرين 10/97 و 05/03 تعود لأسباب أهمها أنه من شروط الإنضمام إلى المنظمة العالمية للتجارة هو المصادقة على إتفاقية **"بيرن"** وهو ما فعلته الجزائر بموجب المرسوم الرئاسي (341/97) بالإضافة إلى تبني أحكام إتفاق جوانب الملكية الفكرية المتعلق بالتجارة، والذي ورد في نص المادة 10 منه أن برامج الإعلام الآلي سواء كانت في صورة برنامج مصدر أو صورة منقوشة فهي محمية على أساس أنها مصنفات أدبية، كما أن الإتفاقية الدولية حول الإجرام المعلوماتي نصت على تجريم الإعتداءات على حق المؤلف والحقوق المجاورة إذا ارتكبت هذه الإعتداءات عن طريق نظام معلوماتي في نطاق تجاري[2].

الفرعالثاني: مواجهة الجريمة المعلوماتية في التشريع المقارن

لقد استدركت أغلب الدول بمختلف أنظمتها القانونية الفشل في ملاءمة القوانين النافذة الإستجابةللإعتداءات الحاصلة على النظم المعلوماتية. وسوف نأخذ في هذا الصدد تجربة المشرع الفرنسي كنموذج قريب من المشرع الجزائري والمشرع الأمريكي ممثلا للنظام الإنكلوسكسوني.

أولا: التشريع الفرنسي: كانت أولى المحاولات لمد سلطان قانون العقوبات لحماية المال المعلوماتي بفرنسا من طرف وزيرها للعدل عام 1985 عندما تقدم بمشروع قانون عقوبات جديد أضاف بموجبه بابا رابعا للكتاب الثالث منه بعنوان "الجرائم في المادة المعلوماتية" Infractions enmatiére informatique، تناول بالتجريم الموضوعات التالية:

- الإلتقاط العمدي للبرامج أو أي عنصر آخر من النظام المعلوماتي.

(1)نص المادة 04 من الأمر 10/97: "تعتبر على الخصوص مؤلفات أدبية أو فنية محمية ما يأتي: المصنفات الأدبية المكتوبة مثل....ومصنفات وقواعد البيانات"

(2) عطا الله فشار. بحث حول مواجهة الجريمة المعلوماتية في التشريع الجزائري كلية الحقوق والعلوم السياسية بجامعة الجلفة. بدون ترقيم

- إستخدام برنامج أو معطيات أو أي عنصر من عناصر النظام المعلوماتي دون موافقة من لهم الحق فيه.
- تخريب أو عرقلة أداء كل أو جزء من نظام المعالجة الآلية للمعلومات.

لكن هذا المشروع لم يكتب له النجاح، و لم يجد سبيله للتطبيق إلى أن تقدم النائب Jacques codfrainفي 1986/08/05 ونواب آخرون في الجمعية الوطنية باقتراح مشروع قانون عن الغش المعلوماتي La fraude informatiqueحاول من خلاله تطويع بعض النصوص القائمة في قانون العقوبات والتي تتناول جرائم تقليدية كالسرقة وخيانة الأمانة والتزوير والإتلاف... وذلك لتشمل العدوان على المال المعلوماتي. وبعد المناقشات في البرلمان أسفرت عن قانون اختلف تماما عن ذلك المشروع الذي قدم لأول مرة بل تشابه إلى حد كبير مع المشروع الأول الذي تقدم به وزير العدل سنة 1985،فصدر بذلك القانون رقم 19 لسنة 1988 المتعلق بحماية نظم المعالجة الآلية للبيانات ثم تم إدراجه في قانون العقوبات لعام 1992 وطبق بعدها في 1994/03/01،وقد تضمن النص على مجموعة من الجرائم في المواد من 2/462 إلى 9/462 وهي:

- الدخول أو البقاء غير المشروع في نظام معالجة آلية المعطيات أو في جزء منه.
- محو أو تعديل المعطيات الموجودة داخل النظام المعلوماتي.
- كل فعل عمدي من شأنه أن يعرقل أو يفسد أداء النظام لوظيفته.
- تزوير المستندات المعالجة آليا أيا كان شكلها واستعمال هذه المستندات.

أما المحطة التالية من محطات التجريم المعلوماتي في فرنسا فكانت عام 2004 عندما(1) أضاف المشرع الفرنسي بموجبه جريمة أخرى هي جريمة التعامل في الوسائل التي تصلح أن ترتكب بها جريمة الدخول أو البقاء غير المصرح بها أو جريمة التلاعب بالمعطيات أو جريمة إعاقة وإفساد أنظمة المعالجة الآلية للمعطيات(2).

---

(1) في عام 1994 تم تعديل قانون العقوبات الفرنسي والذي مس نص المادة 1/441 فطور من جريمة التزوير المعلوماتي لتصبح جريمة تزوير المستندات المعلوماتية واستعمالها بعدما كانت جريمة تزوير المستندات المعالجة آليا فحسب.

(2) القانون رقم 575 لسنة 2004 في 2004/06/21 المتعلق بالثقة في الاقتصاد الرقمي.

ثانيا: التشريع في الولايات المتحدة الأمريكية: يعد قانون فلوريدا لجرائم الحاسوب الصادر عام 1978 أول قانون في الولايات المتحدة الأمريكية يخاطب الجريمة المعلوماتية، حيث يعتبر هذا القانون أن كل دخول إلى الحاسوب غير مصرح به هو بمثابة جريمة، حتى ولو لم تكن هناك نية عدائية من هذا الدخول،[1] أما على الصعيد الفدرالي فقد صدر عام 1984 قانون الإحتيال وسوء استخدام الكمبيوتر ComputerFraudand AbuseACTوقد تم تعديله مؤخرا عام 2001 بمقتضى القانون الوطني المؤرخ في 2001/10/26 وتم إدراجه في القسم 1030من الباب 18 من القانون الفدرالي للولايات المتحدة الأمريكية . وقد عاقبت المادة 1030 من هذا القانون كل من يقوم بالدخول عمدًا إلى حاسوب مشمول بالحماية دون أن يكون مصرحا له بذلك أو يتجاوز التصريح الممنوح له إذا كان الغرض من هذا الدخول هو الحصول على شيء ذي قيمة عن طريق الإحتيال.

وما يمكن الإشارة إليه أن التشريع الفدرالي الأمريكي قبل عام 1986 لم يكن يحتوي على تجريم إتلاف المعلومات و البرامج وإنما اقتصر التجريم على إعاقة أنظمة الحاسبات الآلية . فقد جرمت الفقرة الثالثة من المادة 1030 من القانون الفدرالي لجرائم الحاسبات الآلية الصادر عام 1984 إتلاف المعلومات الذي يترتب عليه إعاقة الحكومة عن استعمال أنظمة الحاسبات الآلية وفي عام 1986 ونتيجة لكثير من الإنتقادات التي وجهت لهذا القانون فقد تم تعديله وأصبحت الفقرة الثالثة من المادة 1030 تتناول فقط الدخول غير المصرح به إلى حاسب آلي تستعمله الحكومة متى أعاق الدخول هذا الإستعمال. وأضيفت فقرة خامسة للمادة 1030 تتناول جريمة الإتلاف العمدي وغير المصرح به لمعلومات يحتوي عليها حاسب آلي تابع للحكومة وإدارتها أو حاسب آلي غير تابع للحكومة إلا أنه يتم استخدامه من طرفها أو لصالحها، أو إعاقة هذا الحاسب عن أداء المهام المختلفة التي تباشرها الحكومة بواسطته، وبصدور قانون حماية بنية المعلومات القومية لعام 1996 تم تعديل المادة السابقة بشكل جوهري، وقد شمل هذا التعديل التوسع في نطاق حماية أنظمة الحاسبات الآلية. فوفقا للفقرة الثانية من المادة 1030 لم تعد الحماية مقصورة على الحاسبات الآلية التابعة للحكومة و إدارتها أو التي يتم استخدامها من قبلها، و إنما اتسعت الحماية

---

(1) محمد طارق عبد الرؤوف الحن، جريمة الإحتيال عبر الأنترنات (الأحكام الموضوعية و الأحكام الإجرائية)منشورات الحلبي الحقوقية الطبعة الأولى 2011ص 104.

لتشمل جميع الحاسبات التي يتم استخدامها من قبل المؤسسات الإقتصادية أو التي تستخدم في التجارة و الإتصالات وهو ما أطلق عليه بالحاسبات التي تتمتع بالحماية.

المطلب الثاني: مواجهة الجريمة المعلوماتية على المستوى الدولي

إن الانتشار الواسع للحواسيب الآلية وشبكات الإتصال الخاصة بها وسع كثيرا من المجال الذي يمكن للجرائم المعلوماتية أن تحدث أثرها فيه. فأصبح هذا النوع المستحدث من الجرائم يعبر الحدود ليلحق الضرر بعدة دول ومجتمعات، و لم يعد يتمركز في دولة معينة ولا يوجه لمجتمع بعينه نتيجة التطور الكبير للوسائل التقنية الحديثة في الإتصالات ودخول جميع فئات المجتمع إلى قائمة مستخدميها فلم يتردد المنحرفون منهم في استغلالها لأغراض دنيئة، وإزاء ذلك كان من الضروري أن تلم الدول شملها وتوحد جهودها في مواجهة هذا الإجرام، وذلك من خلاالسعي إلى تكوين أرضية قانونية تعمل على دعم الكفاح الدولي المشترك ضد الجريمة المعلوماتية وطرح المشاكل والحلول وإعداد مشروعات القوانين تسير على هديها الدول المشتركة، وهو دور المنظمات الدولية والإقليمية لإبرام الإتفاقيات بهذا الخصوص. وسوف نعرض فيما يلي جهود الأمم المتحدة في مواجهة الجريمة المعلوماتية ثم الجهود على المستوى الإقليمي من خلال الاتحاد الأوروبي ومجلس وزراء العدل العرب في هذا المجال.

الفرعالأول: جهود أو دور الأمم المتحدة في مواجهة الجريمة المعلوماتية

تبذل الأمم المتحدة جهودًا لا يستهان بها في مجال محاولة التصدي للجرائم المعلوماتية، وتؤكد على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون على الحد من انتشارها وتعاظم آثارها،[1]وذلك من خلال متابعتها وإشرافها على عقد المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين أو من خلال الوكالات والمنظمات العاملة تحت لوائها.

ففيما يخص مؤتمرات الأمم المتحدة في هذا المجال نجد المؤتمر السابع المنعقد بميلانو عام 1985 الذي كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعالجة الآلية والإعتداء على الحاسب الآلي وإعداد تقرير يعرضه على المؤتمر الثامن، وقد عقد هذا الأخير في هافانا عام 1990وقد خرج

(1) محمود أحمد عبانه. جرائم الحاسوب و أبعادها الدولية دار الثقافة للنشر و التوزيع الطبعة الأولى 2009ص 155.

بالعديد من التوصيات[1] أهمها التأكيد على ضرورة الإستفادة من التطورات العلمية والتكنولوجية في مواجهة الجريمة المعلوماتية، وأشار إلى مسالة الخصوصية واختراقها بالإطلاع على البيانات الشخصية المخزنة داخل النظام المعلوماتي، كما أكد على ضرورة تحديث القوانين التي تتناول هذه الجرائم وتحسين تدابير الأمن والوقاية المتعلقة بها، وتدريب القضاة والمسؤولين على كيفية التحقيق والمحاكمة فيها، وكذا التعاون مع المنظمات المهتمة بهذا الموضوع.

كما عقد مؤتمر الأمم المتحدة لمنع الجريمة ومعاملة المجرمين في القاهرة عام 1995 والذي أوصى بوجوب حماية الإنسان في حياته الخاصة وملكيته الفكرية من تزايد مخاطر التكنولوجيا ووجوب التنسيق والتعاون بين أفراد المجتمع الدولي لاتخاذ الإجراءات المناسبة، كما أوصى كذلك المؤتمر العاشر المنعقد في بودابست عام 2000 بوجوب العمل الجاد من أجل الحد من جرائم تقنية المعلومات المتزايدة والتي اعتبرت نمطا من الجرائم المستحدثة والعمل على اتخاذ تدابير مناسبة للحد من أعمال القرصنة[2].

بالإضافة إلى مؤتمرات الأمم المتحدة نذكر في هذا المجال المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات الذي عقد في ريودي جانيرو عام 1994 وقد خرج بالعديد من التوصيات منها ما يتعلق بوضع قائمة بالحد الأدنى للأفعال المتعين تجريمها واعتبارها من قبيل الجرائم المعلوماتية ووجوب تحديد الجهات التي تقوم بإجراء التفتيش والضبط، وضرورة وضع القواعد المتعلقة بالإثبات الإلكتروني ومصداقية الأدلة[3].

زيادة على جهود الأمم المتحدة من خلال مؤتمراتها التي تعنى بمنع الجريمة ومعاملة المجرمين و التي يقع على عاتقها مهمة مكافحة الجريمة وتقديم المشورة للأمين العام وإيجاد البرامج ووضع الخطط ورسم سياسات لتدابير دولية في مجال منع الجريمة، تلعب الوكالات والمنظمات العالمية العاملة تحت لواء الأمم المتحدة دورًا في هذا المجال ومن ذلك المنظمة العالمية للملكية الفكرية

(1) محمد طارق عبد الرؤوف الحن. المرجع السابق. ص 118.

(2) محمود أحمد عيانة. المرجع السابق. ص 159.

(3) مشار اليه لدى محمد طارق عبد الرؤوف الحن.المرجع السابق. ص 188.

(WIPO) [1]. هذهالأخيرة شكلت مجموعة عمل تضم عددا كبيرا من الخبراء بهدف دراسة الأساليب المناسبة لحماية برامج الحاسب الآلي من خلال إخضاعها لقوانين حماية حق المؤلف.

الفرع الثاني: الجهود الإقليمية في مواجهة الجريمة المعلوماتية

اخترنا للتدليل على هذه الجهود الدور الذي لعبه كل من المجلس الأوروبي والجامعة العربية في إطار المكافحة التشريعية للجريمة المعلوماتية على المستوى الإقليمي.

أولا: دور المجلس الأوروبي: لعب المجلس الأوروبي دورا مهما في محاولة الحد مناالجرائم المعلوماتية، من خلال إقراره العديد من التوصيات الخاصة بحماية البيانات ذات الصبغة الشخصية من سوء الإستخدام وحماية تدفق المعلومات، وفي 1981/01/28 تم توقيع إتفاقية تحت مضلة المجلس الأوروبي تتعلق بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية.

وفي عام 1989 نشر المجلس الأوروبي دراسة تضمنت توصيات تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسب وهي التوصية التي لحقتها دراسة أخرى في عام 1995 حول الإجراءات الجنائية في مجال الجرائم المعلوماتية. وعلى أساس المبادئ التي تضمنتها التوصيات قام المجلس الأوروبي في عام 1997 بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضي وذلك بقصد إعداد إتفاقية في هذا الإطار[2]

ولعل أهم ما قام به المجلس في هذا المجال هو إشرافه على اتفاقية بودابست الموقعة في 2001/11/23[3] . ورغم أن هذه الاتفاقية هي في الأصل أوروبية الميلاد إلا أنها دولية الطابع، لما تظهره من بعد حقيقي عن الإهتمام الدولي بهذه النوعية من الجرائم.وقد تضمنت هذه الاتفاقية 48 مادة غطت في مضمونها ثلاث أقسام كبرى:

([1]) World international propretyorganization.

([2]) وضاح محمود الحمود ونشات مفضي المجالي المرجع السابق، ص 200.

([3]) بتاريخ 2001/11/23 قامت 26 دولة أوروبية بالتوقيع على أول اتفاقية تكافح الجريمة المعلوماتية، كما شاركت أربع دول من غير الأعضاء في المجلس الأوروبي بالمشاركة في إعداد هذه الاتفاقية والتوقيع عليها أيضا وهي كندا اليابان وجنوب إفريقيا والولايات المتحدة الأمريكية. وقد استغرقت المفاوضات بين الدول أربعة أعوام حتى تم التوصل إلى الصيغة النهائية.

- القسم الأول تناول مجموعة الجرائم التي يمكن أن تتعرض لها النظم المعلوماتية[1]
- القسم الثاني: تناول مجموعة الإجراءات الجنائية التي يمكن أن تتخذ في مواجهة هذا النوع من الجرائم خصوصا تفتيش وضبط البيانات المخزنة في الحاسوب.
- القسم الثالث: تناول موضوع التعاون الدولي بين الدول الأعضاء الموقعة على الإتفاقية.

ثانيا: القانون العربي الإسترشادي[2] (النموذجي) لمكافحة الجريمة المعلوماتية:إعتمدت جامعة الدول العربية عبر الأمانة العامة لمجلس وزراء العدل العرب ما سمي بالقانون العربي الإسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها، أين تم اعتماده من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم (495-د 19-2003/10/08) ويعد هذا القانون أبرز الجهود العربية المبذولة في مجال الحماية من الجرائم المعلوماتية من الناحية التشريعية. وقد تضمن هذا القانون 27 مادة موزعة على أربعة أبواب يعالج الباب الأول الجرائم المعلوماتية.

والتي تم النص عليها في المواد من 3 إلى 22 ومن أهمها:

- جريمة الدخول بغير حق إلى موقع أو نظام معلوماتي، مع تشديد العقوبة إذا كان بغرض إلغاء أو إتلاف أو إعادة نشر بيانات أو معلومات شخصية.
- جريمة تزوير المستندات المعالجة في نظام معلوماتي واستعماله.
- جريمة الإدخال الذي من شأنه إيقاف الشبكة المعلوماتية عن العمل، أو إتلاف البرامج أو البيانات فيها.
- جريمة التنصت دون وجه حق على ما هو مرسل عن طريق الشبكة المعلوماتية.

---

(1) تضمنت الإتفاقية أربع طوائف رئيسية للجرائم المعلوماتية وهذه الطرائق هي:

- الطائفة الأول: الجرائم التي تستهدف عناصر أمن المعلومات وهي الجرائم ضد السرية والسلامة ووجود بيانات الحاسوب وتشمل جريمة الدخول غير المشروع- جريمة المراقبة أو الاعتراض غير المشروع- جريمة التشويش على البيانات- جريمة إتلاف نظام الحاسوب.
- الطائفة الثانية: وتشمل التزوير المرتبط بالحاسوب والإحتيال المرتبط بالحاسوب.
- الطائفة الثالثة: الجرائم المرتبطة بالمحتوي وهي جريمة دعارة الأطفال.
- الطائفة الرابعة: وتشمل الجرائم التي تعد اعتداء على المصنفات المحمية.

(2) تم إعداد هذا القانون من قبل لجنة مشتركة بين المكتب التنفيذي لمؤتمر وزراء العدل العرب و المكتب التنفيذي لمؤتمر وزراء الداخلية العرب حيث جرى إقراره بوصفه منهجا استرشاديا للمشرع الوطني عند إعداد تشريع يتعلق بالجرائم المعلوماتية.

- الجرائم المخلة بالآداب العامة عبر الشبكة المعلوماتية.

وتناول الباب الثاني التجارة والمعاملات الإكترونية، أما الباب الثالث فقد تناول حماية حقوق المؤلف عبر الوسائط الإلكترونية في حين عالج الباب الرابع الإجراءات المتعلقة بالجريمة المعلوماتية.

وإن كان القانون العربي الإسترشادي لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها جاء موفقا إلى حد ما في أحكامه الموضوعية حيث شملت بيانا لأهم الجرائم التي يمكن أن ترتكب في مجال الأنظمة المعلوماتية، إلا أنه يؤخذ عليه خلوه من الأحكام الإجرائية الضرورية لملاحقة هذه الجرائم، فلم يتعرض لمسألة الإختصاص القضائي بشكل واضح و لم يشر إلى إخضاع البيانات والمعلومات لإجراءات التفتيش والضبط، و لم يتعرض كذلك لمفهوم الدليل التقني وشروطه وحجيته.

المطلب الثالث: التعــاون الــدولي في مجال مكافحــة الجريمة المعلــوماتية

في العالم الإفتراضي الرحب يمكن أن يقوم شخص بارتكاب جرائم معلوماتية في أثناء وجوده في بلد معين ضد ضحايا قاطنين في بلد آخر مختلف، كما يمكن أن يتم ارتكاب هذه الجرائم في عدد من البلدان في نفس الوقت ومن ذات المنطلق، كما يمكن للأشخاص القائمين على توجيه الجرائم المعلوماتية أن يقوموا بتحريك موقع ارتكاب الجريمة من بلد إلى آخر حتى تستعصي الجريمة على الكشف ويصعب تتبع الجناة، ومن ثمة فإن التقنية المعلوماتية أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بجريمة معلوماتية واحدة في آن واحد.

فالبعد الدولي(1) للجريمة المعلوماتية إذن يفرض على المجتمع الدولي البحث عن وسائل أكثر ملائمة لطبيعة هذه الجرائم لتضييق الثغرات القانونية التي برع مرتكبوها في استغلالها للتهرب من العقاب ولنشر نشاطهم الإجرامي في مناطق مختلفة من أنحاء العالم.

(1)لقد اعتبرت إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنيةالمعتمدة من طرف الجمعية العامة للأمم المتحدة في 2000/11/15في الباب الثالث منها أن أي جريمة تعد جريمة ذات طابع دولي إذا:

- تم ارتكابها في أكثر من دولة.
- تم ارتكابها في دولة ما ولكن جانب كبير من عمليات الإعتداء أو التخطيط أو التوجيه أو الإشراف عليها يتم في دولة أخرى.

وإزاء ذلك كان لابد من تكاتف الدول من أجل مكافحة هذا النوع المستحدث من الجرائم التي لم تعد تتمركز في دولة معينة ولا توجه لمجتمع بعينه، بل أصبحت تعبر الحدود لتلحق الضرر بعدة دول ومجتمعات مستغلة التطور الكبير للوسائل التقنية الحديثة في الإتصالات وتعزيز التعاون بينها واتخاذ التدابير الفعالة للحد منها والقضاء عليها ومعاقبة مرتكبيها(1).

ورغم المناداة بضرورة التعاون الدولي، إلا أن هذا الأمر قد لاق من الصعوبات ما من شأنه الحد من فعاليته بإعاقة الأسس العلمية للتعاون الدولي اللازم والملائم لمكافحة الجريمة المعلوماتية.

وعلى هدي ما تقدم سوف نتناول بالدراسة مظاهر التعاون الدولي ثم بيان الصعوبات التي تواجهه.

الفرع الأول: مظاهر التعاون الدولي في مكافحة الجريمة المعلوماتية:

لقد أثبت الواقع العملي أن أي دولة لا تستطيع بجهودها المنفردة القضاء على الجريمة المعلوماتية، خاصة مع التطور الملموس والمذهل في الإتصالات وتكنولوجيات المعلومات.

فإن كان من الضروري أن تمتلك الدول الإمكانات التشريعية والقضائية والفنية لمكافحة الجريمة المعلوماتية، فان الأهم من ذلك أن تكون تلك القوانين متوائمة و متجانسة بين مختلف الدول، إذ هي تحمي مصلحة مشتركة.

والتعاون الدولي في مجال مكافحة الجريمة المعلوماتية قد يأخذ مظهران، الأول يتعلق بالسعي إلى اتخاذ الإجراءات والآليات ذات الطبيعة التقنية الفنية التي تكفل منع ارتكاب الجريمة في مرحلة التنفيذ. والثاني يتعلق بضرورة التعاون في إنفاذ القانون لملاحقة ومتابعة ومعاقبة المجرمين بعد ارتكاب الجريمة والتي تعبر إختصاصات قضائية متعددة ذات نظم قانونية مختلفة، ويتمثل في التعاون القضائي.

تم ارتكابها في دولة ما ولكن كان لها آثار شديدة على دولة أخرى

(1)حسين بن سعيد بن سيف الغافري. الجهود الدولية في مواجهة جرائم الإنترانت ورقة مقدمة للاتحاد العربي للتحكيم الالكتروني 2007، ص 02.

أولا: التعاون القضائي الدولي في مواجهة الجريمة المعلوماتية:إن التعاون القضائي الدولي يعد الآلية الرئيسية للكفاح ضد الجريمة العابرة للوطنية بأبعادها المختلفة.[1] وفيما يتعلق بالجريمة المعلوماتية فإن فعالية التحقيق والملاحقة القضائية غالبا ما تقتضي الحاجة إلى مساعدة من السلطات في البلد الذي كان منشأً للجريمة، أو من السلطات في البلد الذي عبر من خلاله النشاط المجرم وهو في طريقه إلى الهدف، أو حيث قد توجد أدلة الجريمة، فقد يكون مرتكب الجريمة المعلوماتية من جنسية دولة ما مستعملا في جريمته حواسيب موجودة في دولة أخرى وتقع آثار جريمته في دولة ثالثة. فمن البديهي أن يقف مبدأ السيادة ومشاكل الحدود والولايات القضائية عقبة أمام اكتشاف هذه الجرائم ومعاقبة مرتكبيها، لذا فإن التحقيقات في الجرائم المعلوماتية ومتابعة مرتكبيها قضائيا تؤكد على أهمية المساعدة القضائية المتبادلة بين الدول.

وتعرف المساعدة القضائية الدولية بأنها كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة أخرى بصدد جريمة من الجرائم[2].

ولقد نص المشرع الجزائري في القانون 04/09 على مبدأ المساعدة القضائية الدولية المتبادلة في المادة 16 منه، معتبرا أنه في إطار التحريات والتحقيقات القضائية الجارية لمعاينة الجرائم المعلوماتية يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.وتتخذ المساعدة القضائية الدولية عدة صور أهمها:

1.تبادل المعلومات: يولي المجتمع الدولي لتبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عموما والجريمة المعلوماتية خصوصا لما توفره المعلومات الصحيحة والموثوقة من مساندة لأجهزة تنفيذ القانون. ويشمل مبدأ تبادل المعلومات تقديم البيانات والوثائق والمواد الإستدلالية التي تطلبها سلطة أجنبية وهي بصدد النظر في جريمة معلوماتية ما.

---

(1) أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجرائم ورقة مقدمة في المؤتمر المغاربي الأول، جامعة السابع من أفريل ليبيا. ص 02.

(2) سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية .دكتوراه الحقوق. جامعة عين شمس، 1997، ص 425.

فتميز الجريمة المعلوماتية بالعالمية وبكونها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالإتصال المباشر بين الأجهزة القضائية والأمنية في الدول المختلفة من أجل تبادل المعلومات المتعلقة بالجريمة والمجرمين. ولهذه الصورة من صور المساعدة القضائية صدى كبير في كثير من الإتفاقيات، أهمها ما ورد في الفقرة الثانية من المادة الأولى لمعاهدة الأمم المتحدة النموذجية لتبادل المساعدة في المسائل الجنائية[1] وكذا ما ورد في البند الثالث والرابع والخامس من المادة الثامنة لاتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة الوطنية، إذ أوجبت على الدول الأطراف تيسير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي.

ويصدق الأمر أيضا على ما قضت به المادة الأولى من اتفاقية الرياض للتعاون القضائي العربي بشأن ضرورة تبادل المعلومات بين الدول الأطراف والتنسيق بين الأنظمة القضائية.وفي هذا الإطار أيضا صاغ إتفاقشنغانللإتحاد الأوروبي نظاما متكاملا لتبادل المعلومات[2].

وعلى المستوى التشريعي الوطني فقد نصت المادة 17 من القانون 04/09 على أن الدولة الجزائرية تستجيب لطلبات المساعدة القضائية الدولية الرامية لتبادل المعلومات وذلك في إطار الإتفاقيات الدولية ذات الصلة ومبدأ المعاملة بالمثل.

2- **نقل الإجراءات:** ويقصد بهذه الصورة قيام دولة ما بمقتضى إتفاقيةأومعاهدة باتخاذ إجراءات جنائية وهي بصدد التحقيق في جريمة معلوماتية ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى توفرت مجموعة من الشروط، أهمها التجريم المزدوج والذي يقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب نقل الإجراءات إليها بالإضافة إلى شرعية الإجراءات المطلوب إتخاذها. بمعنى أن تكون مقررة في قانون الدولة المطلوب إليها عن ذات الجريمة وأن تكون هذه الإجراءات ذات أهمية من شانها أن تؤدي دورا مهما في الوصول إلى الحقيقة.

([1]) صدرت هذه المعاهدة في 1990/12/14 في الجلسة العامة 68 للجمعية العامة للأمم المتحدة وتقضي باتفاق أطرافها على أن يقدم كل منهم للآخر أكبر قدر ممكن من المساعدة المتبادلة في التحقيقات أو إجراءات المحاكمة المتعلقة بجرائم يكون العقاب عليها وقت طلب المساعدة داخلا في اختصاص السلطة القضائية للدولة طالبة المساعدة.

([2])Michel quellie : stratigies en France par la police la criminaliteorganisee 1996 p 199

ولقد أقرت العديد من الإتفاقيات الدولية منها والإقليمية هذه الصورة كإحدى صورالمساعدة القضائية الدولية، كمعاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية[(1)] وكذا إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية.

3- **الإنابات القضائية الدولية:** يقصد بهذه الصورة طلب إتخاذ إجراء قضائي من إجراءات الدعوى العمومية تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك عند الفصل في مسألة معروضة لدى السلطة القضائية في الدولة الطالبة لتعذر قيامها بهذا الإجراء بنفسها.[(2)] وتهدف هذه الصورة إلى تسهيل الإجراءات الجزائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية، التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى لسماع شهود أو إجراء تفتيش أو غيرها.

ويحدث بدرجة متزايدة أن تشترط المعاهدات والإتفاقيات الخاصة بتبادل المساعدة القضائية الدولية على الدول الأطراف أن تعين سلطة مركزية عادة ما تكون وزارة العدل ترسل إليها الطلبات مباشرة بدلا من المرور عبر القنوات الدبلوماسية، وذلك بغرض التسريع في الإجراءات وسوف نتطرق لهذه الصورة لاحقا بشيء من التفصيل.

4- **تسليم المجرمين:** استقر الفقه القانوني على اعتبار أن تسليم المجرمين شكل من أشكال التعاون الدولي في مكافحة الجريمة، وهذا النوع من التعاون الدولي هو نتيجة طبيعية للتطورات التي حدثت في كافة المجالات ومنها مجال الإتصالات وتقنية المعلومات، حيث لم تعد الحدود القائمة بين الدول تشكل حاجزا أمام مرتكبي الجرائم، كما أن نشاطهم الإجرامي لم يعد قاصرا على إقليم معين بل امتد إلى أكثر من إقليم، حيث بات المجرم منهم يشرع في التحضير لارتكاب جريمته في دولة معينة ويُقبل على تنفيذها في بلد آخر، وقد يفر إلى بلد ثالث للإبتعاد عن أيدي أجهزة العدالة، فالمجرم المعلوماتي أصبح بالتبعية مجرما دوليا. ولكون أنه لا يمكن لأي دولة أن تجاوز حدودها الإقليمية لممارسة أعمالها القضائية على المجرمين الفارين، كان لابد من إيجاد آلية معينة للتعاون مع الدولة التي ينبغي اتخاذ الإجراءات القضائية فوق إقليمها، تتمثل في تسليم المجرمين

([1]) اعتمدت هذه المعاهدة بموجب قرار الجمعية العامة للأمم المتحدة 45/118 بتاريخ 1990/12/14.

([2]) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنات, دار النهضة العربية للقاهرة ص 83.

الفارين لها. وهذا الإجراء يقوم أساسا على أن الدولة التي يتواجد على إقليمها المتهم بارتكاب جريمة معلوماتية عليها أن تقوم بمحاكمته إذا كان تشريعها يسمح بذلك، وإلا كان عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة. فهو يحقق بذلك مصلحة الدولتين الأطراف في عملية التسليم، إذ يحقق مصلحة الدولة الأولى في كونه يضمن معاقبة الفرد الذي أخل بقوانينها وفي ذات الوقت يحقق مصلحة الدولة الثانية المطلوب إليها التسليم كونه يساعدها على تطهير إقليمها من فرد خارج عن القانون. ولذلك فقد حرصت معظم الدول على سن التشريعات الخاصة بتسليم المجرمين ومنها المشرع الجزائري الذي أخذ بهذا الإجراء كمظهر من مظاهر التعاون الدولي بين السلطات القضائية الأجنبية في قانون الإجراءات الجزائية في المواد 694 وما يليها.

ثانيا: التعاون الفني الدولي في مواجهة الجريمة المعلوماتية:لا يقتصر التعاون الدولي في مجال مواجهة الجريمة المعلوماتية على المساعدة القضائية المتبادلة فحسب، وإنما يشمل كذلك المساعدة التقنية وتبادل الخبرات بين الدول، ذلك أن العنصر البشري سواء على مستوى الأجهزة القضائية أو الأجهزة الأمنية ليس بذات الجاهزية والمستوى لمواجهة الجريمة المعلوماتية، وإنما يختلف من دولة إلى أخرى بحسب تقدم تلك الدولة ورقيها.

ونجد أن جميع الاتفاقيات الدولية أو الإقليمية ذات الصلة قد دعت صراحة إلى ضرورة وجود تعاون دولي في مجال التدريب ونقل الخبرات فيما بينها،[(1)] ذلك أن التقدم المتواصل في تكنولوجيات المعلومات يفرض على الجهات القضائية والأمنية أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنيات والإلمام بها حتى يمكن التصدي للأفعال الإجرامية التي صاحبت هذه التكنولوجيا ومن ناحية أخرى فإن إعمال القانون في مواجهة الجرائم المعلوماتية يستلزم اتخاذ إجراءات قد تتجاوز المفاهيم والمبادئ المستقرة في المدونة العقابية التقليدية لما تتسم به هذه الجرائم من حداثة في الأسلوب وسرعة في التنفيذ وسهولة في إخفائها ومحو آثارها، وبالتالي فإن ظهور هذه الأنماط الجديدة من الجرائم أصبح يشكل عبئا ثقيلا على عاتق الأجهزة القضائية المختصة من قضاة تحقيق وقضاة حكم. وكذا رجال الضبطية القضائية،لأجل ذلك كان لابد أن تكون تلك الأجهزة على مختلف أنواعها على درجة كبيرة من الكفاءة والمعرفة والقدرة في التعامل

([1]) انظر المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والمادة 09 من مشروع الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود.

مع الجريمة المعلوماتية والمجرم المعلوماتي. ومن هذا المنطلق كانت الدعوى إلى ضرورة وجود تعاون دولي في مجال تدريب رجال القضاء والضبطية القضائية للاستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء ومؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بوسائل سهلة ميسرة.

و التدريب المقصود هنا ليس التدريب التقليدي فحسب، فلا يكف أن تتوافر لدى رجال القضاء الخلفية القانونية، ولدى الضبطية القضائية خصائص عمل الشُرطيوإنما لابد من إكسابهم خبرة فنية في مجال الجريمة المعلوماتية. وهذه الأخيرة لا تتأت دون تدريب تخصصي يراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب.

أما بالنسبة للمنهج التدريبي فيجب أن يشمل على بيان بالمخاطر والتهديدات ونقاط الضعف وأماكن الإختراقات لشبكة المعلومات وأجهزة الحاسب الآلي وتحديد أنماط ونوعية الجرائم المعلوماتية، وبيانا لأهم الصفات التي يتميز بها المجرم المعلوماتي والدوافع وراء ارتكابه للجريمة المعلوماتية. وفيما يتعلق بمنهج التدريب على التحقيق في الجريمة المعلوماتية فإنه لابد أن يشتمل على إجراءات التحقيق، التخطيط للتحقيق، تجميع المعلومات وتحليلها، أساليب المواجهة والاستجواب، طرق مراجعة النظم الفنية للمعلومات وأساليب المعمل الجنائي. بالإضافة إلى ما يتعلق بالتفتيش والضبط وكيفية استخدام الحاسب الآلي كأداة للمراجعة والحصول على الأدلة(1).

وصفوة القول وخلاصته أنه ما من دولة يمكنها مجابهة هذا التحدي في مواجهة الجريمة المعلوماتية بمفردها، فلا مفر إذن من مواصلة تطوير القدرة على التعاون الدولي في المجال التدريبي والتبادل التقني من خلال قيام الدول المتقدمة تقنيا وتكنولوجيا ولها صيت كبير في مواجهة الجرائم

---

(1) هشام محمد فريد رستم. الجرائم المعلوماتية. أصول التحقيق الجنائي الفني. بحث مقدم لمؤتمر القانون والكومبيوتر والانترنات- كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة في الفترة 2005/03/01 الطبعة الثاني 2004 ص 496.

المعلوماتية بمساعدة الدول النامية لتعزيز مؤسساتها المتخصصة بالتحري والتحقيق والمحاكمة بتوفير سائر أنواع المعونة التقنية[1].

الفرع الثاني: الصعوبات التي تواجه التعاون الدولي في مكافحة الجرائم المعلوماتية:

رغم المناداة بضرورة التعاون الدولي في مجال مكافحة الجريمة المعلوماتية والذي بات مطلبا تسعى إلى تحقيقه أغلب الدول، إلا أنه ثمة صعوبات ومعوقات تجعل هذا التعاون ليس بالأمر اليسير وذلك كما يلي:

1/ عدم وجود نموذج موحد للنشاط الإجرامي: إذ لم تتفق الأنظمة القانونية في بلدان العالم علىصورة محددة ونماذج معينة يتم الاتفاق المشترك بين الدول حولها تندرج في إطار الجريمة المعلوماتية،[2] فما يكون مجرما في بعض الأنظمة قد لا يكون كذلك في أخرى.

ولعل عدم الاتفاق بين الأنظمة القانونية المختلفة على صور موحدة للسلوك الإجرامي في الجريمة المعلوماتية يغري قراصنة الحاسب الآلي على ارتكاب جرائمهم دون تقيد بالحدود الجغرافية[3].

2/ اختلاف النظم القانونية الإجرائية :إذ بسبب هذا الاختلاف قد تكون هناك طرق للتحري والتحقيق والمحاكمة التي تثبت فعاليتها في دولة ما، قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها كما هو الحال مثلا بالنسبة للمراقبة الإلكترونية، فإذا ما اعتبرت أن طريقة ما من طرق جمع الإستدلالات أو التحقيق أنها قانونية في دولة معينة، قد تكون ذات الطريقة غير مشروعة في دولة أخرى. بالإضافة إلى أنه قد لا تسمح دولة ما باستخدام دليل إثبات جرى جمعه بطرق ترى هذه الدول أنها طرق غير مشروعة.

---

(1) يعمل مكتب المساعدة والتدريب على التحقيق الجزائي (ICITAP) التابع لوزارة العدل الأمريكية على تطوير أجهزة الإدعاء العام في الخارج وعلى توفير مساعدات لأجهزة الشرطة في البلدان النامية.

(2) عبد الفتاح بيومي حجازي الإثبات الجنائي في جرائم الكوبيوتر والانترنات.دار الكتب القانونية. مصر 2007.ص 188

(3) مثال ذلك قضية فيروس (Love Bug) الذي بعد تتبعه من طرف مكتب التحقيقات الفدرالي تبين مصدره الفلبين وأن هوية المعتدي هو أونيل دي جوزمان الذي قام بابتكار هذا الفيروس وتحميله على شبكة الانترنات ونشره في جميع أنحاء العالم ورغم أن هناك أدلة كافية ضد أونيلجوزمان فقد واجه مكتب الإدعاء العام بالفلبين عقبات كبيرة في توجيها لاتهام لعدم وجود قانون في الفلبين لمكافحة القرصنة الالكترونية. و لم يكن بالإمكان محاكمته في بلد آخر على أساس معاهدة تسليم المجرمين مع الفلبين لأن شرط التجريم المزدوج غير متوفر.

3/التجريم المزدوج: يعتبر التجريم المزدوج من أهم شروط تسليم المجرمين، وقد يكون هذا الشرط عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجريمة المعلوماتية، سيما وأن معظم الدول ما زالت نصوصها العقابية خالية من هذا النمط الإجرامي.

وفي الحقيقة فإن المصلحة المشتركة للدول تقتضي البحث عن الوسائل التي تساعد في التغلب على هذه الصعوبات وإيجاد تعاون دولي حقيقي يتفق مع طبيعة هذا النوع المستحدث من الجرائم للتخفيف من خلو الفوارق بين الأنظمة القانونية العقابية الداخلية.

المطلبالرابع: قواعد الاختصاص القضائي في الجرائم المعلوماتية

إن المقصود بالإختصاص القضائي هو السلطة السيادية للدولة التي تمكنها من تطبيق قوانينها الوطنية داخل إقليمها.

وتعد الجرائم المعلوماتية من أكثر الجرائم التي تطرح مسألة الإختصاص القضائي، ذلك أن السلوك أو النشاط الإجرامي فيها لا يعترف بالحدود، فالعالم كله مرهون بمجرد نقرة بسيطة على لوحة مفاتيح جهاز الحاسوب، إذ أن الطبيعة التقنية العالية لنظم المعلوماتية المرتبطة بشبكات الإتصال العالمية يمكن أن تؤدي إلى أن يصبح إقليم أكثر من دولة مسرحا لجريمة واحدة،[1] الأمر الذي قد ينجم عنه تنازع في الإختصاص بين هذه الدول. فقد يحدث أن ترتكب الجريمة المعلوماتية في إقليم دولة معينة وتتحقق النتيجة الجرمية في دولة أخرى، ومن ثم تتعدد القوانين التي يمكن أن تحكم هذه الجرائم بتعدد الدول المرتبطة بها.

وإذا كان الإختصاص على المستوى الداخلي (الوطني) لا يثير أي إشكال، إذ يتم الرجوع في تحديده إلى المعايير المحددة سلفا في قانون الإجراءات الجزائية[2]. فإن المشكلة تثار بالنسبة للإختصاص على المستوى الدولي بين الدول، حيث اختلاف التشريعات والنظم القانونية. والمعروف أن تحديد القانون الواجب التطبيق يترتب عليه تحديد المحكمة المختصة لذلك فإن المسألة تقتضي منا معرفة المبادئ أو المعايير التي يُعتمد عليها في تحديد القانون الواجب التطبيق على الجرائم المرتكبة، وبالتبعية تحديد الولاية أو الاختصاص القضائي ثم نحاول إبراز أثر ذاتية أو خصوصية الجريمة المعلوماتية في تحديد الإختصاص القضائي.

الفرع الأول: قواعد تحديد القانون الواجب التطبيق

إن قواعد القانون الجنائي (بشقيه الموضوعي والإجرائي) تعد مظهرا من مظاهر سيادة الدولة لذلك فإن تطبيقها من حيث المكان يخضع لمبدأ مستقر ألا وهو مبدأ الإقليمية، والذي يعني خضوع

---

(1) عادل عزام سقف الحيط. جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونيةدار الثقافة للنشر والتوزيع الطبعة الأولى، 2011 عمان ص 349.

(2) مكان وقوع الجريمة، مكان محل إقامة المتهم،مكان إلقاء القبض على المتهم.

الجرائم التي تقع في إقليم دولة معينة لقانونها الجنائي النافذ، بحيث تصبح محاكمها هي صاحبة الولاية بنظر الدعوى الناشئة عنها ولا تخضع لسلطان أي قانون أجنبي، وفي المقابل فلا مجال لأن يمتد سريان قانون الدولة الجنائي خارج نطاقها الإقليمي وفقا لحدودها المعترف بها، حيث يصطدم بسيادة غيرها من الدول، إلا في أحوال إستثنائيةتقتضيها حماية المصالح الجوهرية للدولة أو متطلبات التعاون الدولي في مكافحة الإجرام[1].

والأصل أن عناصر الركن المادي للجريمة تكتمل في نطاق إقليم دولة واحدة، حيث يقع السلوك الإجرامي وتترتب عليه آثاره في إقليم دولة واحدة، بيد أن بعض الجرائم يتجاوز مداها أحيانا حدود الدولة، حينما يتجزأ ركنها المادي أو يتوزع على أكثر من مكان، بحيث يمكن وقوع السلوك في إقليم دولة بينما تتحقق النتيجة للجريمة في إقليم دولة أخرى، ويتجلى ذلك في عدد من الجرائم ذات الطبيعة العابرة للحدود الوطنية.

وهذا ما يقود إلى التساؤل عن مكان وقوع الجريمة في هذه الحالة من أجل تحديد القانون الواجب التطبيق. فهل هو مكان السلوك الإجرامي أم المكان الذي تحققت فيه النتيجة؟

إنقسم الرأي بخصوص هذه المسألة إلى ثلاث اتجاهات، فذهب الاتجاه الأول إلى أن العبرة في تحديد مكان وقوع الجريمة بالمكان الذي وقع فيه السلوك الإجرامي بغض النظر عن المكان الذي تحققت فيه نتيجته أو من المفترض تحققها فيه،[2] وفي المقابل ذهب اتجاه آخر إلى أن[3] مكان وقوع الجريمة يتحدد بالمكان الذي تحققت فيه النتيجة أو كان من المفترض تحققها فيه، وبين هذا وذلك انبرى اتجاه ثالث إلى أن العبرة تكون بمكان حصول أي منهما[4].

(1) عدنان الخطيب. موجز القانون الجزائي. الكتاب الأول. المبادئ العامة في قانون العقوبات. مطبعة جامعة دمشق، 1963، ص 79.

(2) حظي هذا الاتجاه بتأييد جانب كبير من الفقه وقد أخذ به المشرع الفرنسي و المصري.

(3)تم تبني هذا الاتجاه من طرف المشرع الألماني الصادر في 1975/12/05، و المشرع التركي في سنة 1982

(4)أقر هذا الاتجاه، المشرع النرويجي، المشرعالإيطالي. المشرع الدانماركي، ونجد أن المشرع الجزائري قد نص في المادة الثانية من قانون العقوبات أنه يطبق قانون العقوبات الجزائري على كافة الجرائم التي ترتكب في أراض الجمهورية كما نصت المادة 586 من قانون الإجراءات الجزائية أنه تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها لها قد تم في الجزائر.

و بالإضافة إلى مبدأ الإقليمية فإن القانون الواجب التطبيق يمكن أن يتحدد أيضا وفقا لمعايير أو مبادئ أخرى،كمبدأ الشخصية أومبدأ العينية أو مبدأ العالمية وغالبا ما تأخذ بها التشريعات الجنائية كمبادئ احتياطية أو مكملة لمبدأ الإقليمية.

والمقصود بمبدأ الشخصية هو تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة ولو ارتكب الجريمة خارج إقليمها، فيخضع حسب هذا المبدأ المواطن لقانون بلاده أينما وجد. وأما مبدأ العينية فيقصد به تطبيق القانون الجزائي على الجرائم التي تمس المصالح الأساسية للدولة والمرتكبة خارج إقليمها أيا كانت جنسية مرتكبها.

ومبدأ العالمية فهو أن تختص الدولة بتطبيق قانونها الجزائي على أجنبي ارتكب جريمة في الخارج وتم توقيفه أو إلقاء القبض عليه بأراضيها.

والمشرع الجزائري قد أخذ بهذه المبادئ حينما نصت المادة الثالثة من قانون العقوبات على أنه يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراض الجمهورية وهو مبدأ الإقليمية موضحا مكان ارتكاب الجريمة خلال نص 586 من قانون الإجراءات الجزائية. إذ تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر.

كما أخذ المشرع الجزائري بمبدأ العينية في نص المادة 588 من قانون الإجراءات الجزائية والتي تنص على أن كل أجنبي ارتكب خارج الإقليم الجزائري بصفته فاعل أصلي أو شريك جناية أو جنحة ضد سلامة الدولة الجزائرية... تجوز متابعته ومحاكمته وفقا للقانون الجزائري إذا ألقي عليه القبض في الجزائر أو حصلت الدولة على تسليمه لها.

وأخذ المشرع أيضا بمبدأ الشخصية من خلال نص المادة 582 من قانون الإجراءات الجزائية التي نصت على أن كل واقعة موصوفة بأنها جناية معاقب عليها في القانون الجزائري ارتكبها جزائري خارج إقليم الجمهورية يجوز أن يتابع ويحاكم في الجزائر.

أما مبدأ العالمية فإن المشرع الجزائري قد اتبع خطة معظم التشريعات العقابية و لم يأخذ به مقتصرا على المبادئ السالفة الذكر[1].

الفرع الثاني: أثر خصوصية الجريمة المعلوماتية على مسألة الإختصاص القضائي:

إن ما تتميز به الجريمة المعلوماتية من طابعها المتخطي لحدود الدولة الواحدة واتسامها بالبعد الدولي وكذا يتجرد السلوك الإجرامي فيها من ناحية خاصيته المادية كان له الأثر الظاهر في وجود صعوبة عند تحديد الاختصاص، بل فرض غموضا في تحديد معياره.

فقد يحدث أن ترتكب جريمة من الجرائم المعلوماتية في إقليم دولة معينة من طرف أجنبي، فتكون الجريمة هنا خاضعة للإختصاص الجنائي للدولة التي ارتكبت الجريمة في إقليمها استنادا إلى مبدأ الإقليمية، وكذا لاختصاص الدولة التي ينتمي إليها الجنائي انطلاقا من مبدأ الشخصية، وقد تُلحق هذه الجريمة تهديدا لأمن وسلامة دولة أخرى، فتدخل أيضا في اختصاصها استنادا إلى مبدأ العينية، وهو الأمر الذي قد يترتب عليه تنازع في الاختصاص بين هذه الدول[2].

للتغلب على التنازع الإيجابي للاختصاصذهب الفقه الجنائي إلى إيجاد حل يتمثل في محاولة إعطاء الأولوية لأي من الدول المتنازعة وفقا لأحد معايير الإختصاص الذي يكون الأكثر جدوى وفعالية لضمان سرعة ملاحقة الجريمة، وقد يكون مبدأ الإقليمية الأكثر قبولا، وذلك أن الدولة التي تقع في إقليمها الجريمة كلها أو الجزء الأكبر من النشاط المكون لركنها المادي هي أرجح الدول اختصاصا بملاحقة الجريمة ومحاكمة فاعلها.ولا يجد هذا الحل مبررا في اعتبارات السيادة الوطنية اللصيقة بمبدأ الإقليمية وإنما يجد مبرره في جدواه العملية، وأنه حيث تقع الجريمة المعلوماتية تصبح أدلة الإثبات متوافرة ويغدو من اليسير إجراء التحقيقات الكفيلة لإظهار الحقيقة.

---

(1) علي عبد الله سليمان. شرح قانون العقوبات الجزائري- ديوان المطبوعات الجامعية .ص 115.

(2) جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنت. دار الفكر العربي.القاهرة 2001، ص 73.

ولقد شهد مفهوم الإقليمية تطورا ملحوظا فيما يتعلق بتحديد مكان وقوع الجريمة المعلوماتية فلم يعد يلازم وقوع فعل مادي أو حتى أحد العناصر المكونة لهذا الفعل، بل بلغ الأمر حد نزع الصفة المادية كلية عن هذا الفعل[1].

وتطبيقا لذلك فقد ذهب القضاء الفرنسي إلى القول بتطبيق القانون الفرنسي وبالتالي اختصاص المحاكم الفرنسية إذا كان مركز البث أو الجهاز الخادم موجودا خارج الإقليم الفرنسي بينما تظهر الرسائل التي يقوم ببثها هذا الجهاز في فرنسا، واعتبر أن الجريمة مرتكبة في كل مكان تظهر فيه هذه الرسائل المؤثمة محل البث[2]. ووفقا لهذا الإتجاه الموسع لمفهوم مبدأ الإقليمية فإن هناك من اعتبر أن الاختصاص القضائي في الجريمة المعلوماتية يؤول للدولة التي يوجد بين إقليمها والجريمة علاقة فعلية وجوهرية[3].

ومن التشريعات المقارنة التي تتجه إلى التوسع في مفهوم الإقليمية التشريع الأمريكي الذي يعطي الإختصاص لمحاكمه الجنائية بمجرد حدوث آثار الجريمة على إقليمها. فقد قضي في أمريكا بأنه إذا تم إدخال بيانات من مكان معين وكانت تتضمن ما يشكل جريمة معلوماتية، وكانت هذه البيانات مقروءة في مكان آخر، (دولة أخرى) فإن الإختصاص ينعقد لمحاكم الدولة التي يمكن الإطلاع على تلك البيانات في إقليمها، فإذا كان الجاني قد وضع صورا مؤثمة على جهاز الخادم المتواجد في إيطاليا وكانت هذه الصور متاح الإطلاع عليها في الولايات المتحدة الأمريكية فإن القضاء الأمريكي يحكم إختصاصه.

وعلى الرغم من اختلاف القوانين المقارنة في تحديد المحكمة المختصة عندما تمر الرسالة الإلكترونية المعاقب عليها في إقليم أكثر من دولة، وكان القانون يعاقب عليها في جميع تلك الدول، فإن الحل الأنسب عند بعض الفقه الجنائي[4] هو أن يؤول الإختصاص لجميع هذه الدول، وذلك ما دامت النتيجة تتحقق في بلد آخر غير بلد تحميل الرسالة وإدخالها على الشبكة

([1]) مفتاح بوبكر المطردي. ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان في 23-2012/09/25.بدون ترقيم.

[2]TGI paris 13. Nov.1998- lionelthoumyve. Hébergement à l'étranger voie sans ssue.op.cit.p2.

([3]) القضاء الكندي:Affaire libman contre la reine

([4])شيماء عبد الغني محمد عطا الله . الحماية الجنائية للتعلملاالالكترونية. دار الجامعة الجديدة. مصر 2007، ص 376.

المعلوماتية، من ذلك أن يرسل المتهم برنامجا من برامج الفيروسات من جهاز يقع في دولة معينة إلى جهاز آخر يقع في دولة ثانية مرورا بجهاز ثالث ورابع في دول أخرى وبالتالي تختص محاكم الدولة التي حدث منها البث والدولة التي انتهى إليها الفيروس والدول التي مر بها هذا الفيروس بجهاز فيها.

وحتى لا يُترك أمر مسألة الإختصاص لمحض اجتهادات الفقه والقضاء كان من اللازم تحديد الموقف القانون الدولي منها من خلال الإتفاقيات الدولية والإقليمية. ففي هذا الإطار يمكن استخدام إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية لتكون أساسا لاتخاذ التدبير اللازمة للحصول على الولاية القضائية على الجرائم المعلوماتية، فقد حددت المادة 15 من هذه الإتفاقية المعايير التي بموجبها يمكن للأطراف المتعاقدة الحصول على الولاية القضائية على الجرائم التي تشملها أحكام هذه الإتفاقية. ومن ذلك نصت هذه المادة على أنه يتعين على كل دولة طرف أن تعتمد ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المقررة في الحالات الآتية:

- عندما يرتكب الجرم في إقليم تلك الدولة.
- عندما يرتكب الجرم ضد أحد مواطني تلك الدولة.
- عندما يرتكب الجرم أحد مواطني تلك الدولة أو شخص عديم الجنسية مكان إقامته المعتاد في إقليمها.

كما نصت أيضا أنه إذا أبلغت الدولة التي تمارس ولايتها القضائية بمقتضى المعايير السابقة أو علمت بطريقة أخرى أن دولة واحدة أو أكثر تجري تحقيقا أو تقوم بملاحقة قضائية بشأن السلوك ذاته فعلى السلطات المختصة في هذه الدول أن تتشاور في ما بينها لهدف تنسيق ما تتخذه من تدابير.

وعلى المستوى الأروبي فثمة إتفاقية مجلس أوروبا لمكافحة الجريمة المعلوماتية التي أوردت في المادة 22 من الباب الثالث من هذه الاتفاقية مسألة الإختصاص بنصها على أنه يعتمد كل طرف ما قد يلزم من تدابير تشريعية، وذلك لإقرار الإختصاص بشأن أي جريمة معلوماتية وذلك عندما ترتكب الجريمة:

- في إقليمه.
- من جانب أحد مواطنيه إذا كانت الجريمة معاقبا عليها بموجب القانون الجنائي بمكان ارتكابها أو في حالة ارتكاب الجريمة خارج الإختصاص القضائي الإقليمي لأي دولة.

بالإضافة إلى أن هذه الإتفاقية لا تستبعد أي اختصاص جنائي يمارسه أحد الأطراف وفقا لقانونه الوطني، وفي حالة مطالبة أكثر من طرف من الأطراف بالإختصاص القضائي بشأن أي جريمة معلوماتية تقررها هذه الاتفاقية، يقوم الأطراف متى كان ذلك ملائما بالتشاور لغرض تحديد الإختصاص القضائي الأكثر ملائمة للمحاكمة.

وعلى هدي ذلك فإن المشرع الجزائري تدخل فعلا بموجب القانون 04/09 في المادة 15 منه الواردة في الفصل السادس بعنوان التعاون و المساعدة القضائية الدولية و الاختصاص القضائي حيث اعتبر المشرع أنه و بالاضافة إلى قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية فإن المحاكم الجزائرية تكون مختصة أيضا بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال المرتكبة خارج الوطن عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجيةللإقتصاد الوطني.

غير أن هذا النص ماهو إلا تكرار لقاعدة الإختصاص العيني المنصوص عليها بالمادة 588 من قانون الإجراءات الجزائية و ليس بالإضافة الجديدة إلى قواعد الإختصاص مثلما استهل به نص المادة15 من القانون 04/09

وصفوة القول فإن الجرائم المعلوماتية العابرة للوطنية تستعصي في كثير من الأحيان على الخضوع للقوالب القانونية التي تحكم مسألة الإختصاص المكاني ومن ثمة فإن الطبيعة الخاصة لهذا الصنف من الجرائم المستحدثة تتطلب تجاوز القوالب والمعايير التي طرحها الفقه التقليدي بخصوص مسألة تنازع الإختصاص والعمل على تبني حلول أكثر مرونة تأخذ في الحسبان النطاق الجغرافي لهذه الجرائم وسهولة ارتكابها وآلية اقترافها والتخلص من آثارها وما إلى ذلك من اعتبارات يفرضها الطابع التقني المتطور لها.

وترتيبا على ما سبق فإن الجريمة المعلوماتية جريمة مستحدثة تستهدف الإعتداء على المعطيات بدلالتها التقنية الواسعة أو الاستعانة بها لإرتكاب جرائم تحاكي الجرائم التقليدية في العالم الافتراضي، وفي هذا الفصل تم تناول أهم التعريفات التي وضعها الفقه الجنائي للجريمة المعلوماتية وذلك حسب الإتجاهات الفقهية التي عنيت بدراسة هذه الجريمة، ثم بعد ذلك تم تحديد الطبيعة القانونية لها ثم تبيان خصائصها وخصائص مرتكبيها، بالإضافة إلى أساليب وتقنيات ارتكابها، ثم تم التعريج بعد ذلك إلى استيضاح موقف التشريع الجزائي من الجريمة المعلوماتية من خلال تسليط الضوء على كيفية المواجهة التشريعية الموضوعية لهذه الجريمة وذلك على مستوى التشريع الجزائري أو المقارن، وكذا الجهود الدولية المبذولة في هذا الإطار، وفي الأخير تم إبراز أهم المشكلات القانونية التي تثيرها هذه الجريمة وهي مشكلة الإختصاص القضائي و القانون الواجب التطبيق باعتبارها جريمة عابرة للوطنية.

الفصـــل الثاني

الجوانب القانونية للتحقيق و إجراءات جمع الدليل في الجريمة المعلوماتية

إن طبيعة الجرائم المعلوماتية بعناصرها ووسائل إرتكابها قد تدفع المشرع الجزائي إلى ان يعيد النظر في كثير من المسائل الإجرائية، خاصة يتعلق فيما يتعلق بمسألة الإثبات باعتبارها أهم موضوعات هذا القانون. ذلك أن الدليل الذي قد يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعتها التقنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية لإستخلاص الدليل قادرة على القيام به. مما يستوجب تدخل المشرع لتكريس قواعد إجرائية يمكن للجهات المكلفة بالبحث والتحري عن الجريمة المعلوماتية الإعتماد عليها في الوصول إلى الدليل المناسب في إثبات الجريمة المعلوماتية.

ولا شك أن هذا الدليل سيتم استخلاصه من البيئة الرقمية، والتي تعتبر مسرح الجريمة المعلوماتية مما يجعله يتميز بخصائصها (خصائص البيئة الرقمية).وهو الأمر الذي يقودنا الى الحديث عن مسالة قبول هذا الدليل أمام القضاء و مدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التزييف والتحريف و الأخطاء، بل وحتى مع ضمان مصداقية هذا الدليل وكذا مشروعيته فإن الأمر لا يتوقف عند هذا الحد، بل يتجاوزه إلى مسألة أكبر أهمية تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية للسلطة التقديرية للقاضي إعمالا لمبدأ الإقتناع الشخصي للقاضي الجزائي الذي يشكل جوهر أي حكم. وسوف أحاول أن أتناول هذه المسائل بنوع من التفصيل.

المبحثالأول: التحقيـــق في الجـــريمة المعلـــوماتية:

إن التحقيق هو إجراء من أهم الإجراءات التي ُتتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل إسمه عليه إستجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة.

والثابت أن الدعوى الجزائية تمر بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بمرحلتين أيضا، مرحلة التحقيق الأولي ومرحلة التحقيق الإبتدائي. فالمرحلة الأولى وهي مرحلة جمع الإستدلالات التي يباشرها أعضاء الضبط القضائي[(1)]، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق[(2)]. وإننا نؤيد الرأي أو الاتجاه[(3)]الذي يقسم التحقيق إلى:

-تحقيق أولي و الذي يناط به رجال الضبطية القضائية.

- تحقيق قضائي ويناط به رجال القضاء، وهذا الأخير يقسم إلى تحقيق ابتدائي من اختصاص قاضي التحقيق وتحقيق نهائي ويكون في مرحلة المحاكمة من طرف قضاة الحكم.

وفي كل جميع أنواع التحقيق هذه، يكون للقائمين عليه من ضبطية قضائية وقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية. وهو الأمر الذي يفهم صراحة من خلال استقراء نص المادتين 12و38 من قانون الإجراءات الجزائية الواردتين في الباب الأول من هذا القانون تحت عنوان" في البحث والتحري عن الجرائم" حيث تنص المادة 12 الفقرة الثالثة أنه "يناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون

---

(1) حسب المادة 15 من قانون الإجراءات الجزائية "يتمتع بصفة ضابط الشرطة القضائية:

- رؤساء البلديات، ضباط الدرك الوطني، محافظوا الشرطة، ضباط الشرطة، ذوو الرتب في الدرك الوطني، ورجال الدرك الذين أمضوا في سلك الدرك أكثر من ثلاث سنوات ويتم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع. مفتشو الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة ثلاث سنوات على الأقل وعينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية وكذا ضباط الصف التابعين للمصالح العسكرية.

(2)يبدو لنا أن المشرع لا يفرق بين التحقيق الأولي والتحقيق الابتدائي وذلك من خلال نص المادة 63 من قلنون الإجراءات الجزائية التي تنص على أن ضباط الشرطة القضائية يقومون بالتحقيقات الابتدائية ..." وفي نفس الوقت تنص المادة 66 الواردة في الباب المتعلق بالأحكام الخاصة بقاضيالتحقيق على أن التحقيق الابتدائي في الجنيات وجوبي وهو بذلك يعتبر أن التحقيق الذي يمارسه سواء رجال الضبطية القضائية أم قضاة التحقيق يعد تحقيقا ابتدائيا على حد السواء.

(3) زهير كاظم عبود، بحث مقدم للأكاديمية العربية المفتوحة في الدنمارك، كلية القانون والسياسة قسم القانون الدراسات العليا 2007 بدون ترقيم.

العقوبات..." وتنص في نفس الوقت المادة38 من نفس القانون أنه "يناط بقاضي التحقيق إجراءات البحث والتحري ..."

وعليه فإنه يمكن القول أن إجراءات البحث و االتحري عن الجرائم هي من صلاحيات جهات التحقيق سواء كان أوليا أم ابتدائيا، وبهذا المفهوم فإن إجراءات البحث و التحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولي، بينما هذه الاجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا إبتدائيا.

وإذا كان التحقيق عموما يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه،وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإضهار الحقيقة، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا تطويرًا لأساليبه وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في هذه البيئة.

المطلب الأول: الأجهزة المكلفة بالبحث والتحري عن الجريمة المعلوماتية:

لقد كان للتزايد المستمر للجرائم المعلوماتية الأثر البالغ في ضرورة تطوير أجهزة الضبط القضائي لتواكب التطور الحاصل في مجال الجريمة، ونتيجة لهذا التحدي قامت معظم الدول بإحداث أجهزة متخصصة بمكافحة هذا النوع من الإجرام المستحدثتتولى مهمة التحري عن جرائم العالم الافتراضي وكشف النقاب عنها، وقدحملت هذه الاجهزة تسميات مختلفة منها مثلا شرطة الانترنت أو فرقة التحري عن جرائم المعلوماتية إلى غير ذلك من التسميات.

ولا يقتصر دور هذه الأجهزة على المستوى الوطني فقط، بل هناك أجهزة متخصصة على المستوى الدولي أيضا.وسوف نستعرض أهم هذهالأجهزة سواء على المستوى الداخلي أو الدولي وذلك كما يلي:

الفرع الأول: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الداخلي:

لقد ظهرت العديد من الأجهزة والهيئات المختصة في مجال الجريمة المعلوماتية في إطار مكافحتها والبحث والتحري عنها وعن مرتكبيها سواء على المستوى الوطني أم على صعيد الدول الأجنبية.

إنه بالنظر إلى الطبيعة التقنية التي تتميز بها الجريمة المعلوماتية ذهبت أغلب الأنظمة القانونية الإجرائية في التشريعات المقارنة ألى أن تعهد بمسألة البحث والتحري عن هذا النوع من الجرائم لأجهزة متخصصة، لها من الكفاءة والتدريب والوسائل البشرية والماديةما يؤهلها للتعامل مع هذا النوع المستحدث من الإجرام.وسوف نحاول أن نلقي الضوء على هذه الأجهزة الموجودة في بعض الدول ثم نعرج على الوضع في بلادنا.

أولا: الأجهزة المختصة في الدول الأجنبية:كانت الدول المتقدمة سباقة بإحداث هذه الأجهزة إذ أن مكافحة الجرائم المعلوماتية مرتبط بمدى تقدم الدول من الناحية التقنية وبمدى توفر الإمكانات المادية اللازمة لإنشاء هذه الأجهزة ونذكر على سبيل المثال في هذا الصدد الدول التالية:

1/الولايات المتحدة الأمريكية: قامت الولايات المتحدة الأمريكية بإنشاء عدة أجهزة لمكافحة الجريمة المعلوماتية ومنها:

- **شرطة الواب webpolice:** وتعتبر نقطة مراقبة على الأنترنات إضافة إلى أنها تتلقى الشكاوى من مستحدميالشبكة وملاحقة الجناة والقراصنة،والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة[1].
- **مركز تلقي شكاوى جرائم الأنترنات IC3**[2]والذي تم إنشاؤه من طرف مكتب التحقيقات الفدرالي FBIفي سنة 2000 .ثم في عام 2003 تم دمج مركز شكاوى الإحتيال عبر الأنترنات المعروف بـــ IFCC[3] مع هذا المركز. ويعمل مركز IC3بصورة تشاركية مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاءNWC،[4]ويقوم هذا المركز بتلقي الشكاوي عبر موقعه على الأنترنات أين يقوم الشاكي بملئ إستمارة إلكترونية ثم يقوم المختصون في هذا المركز بتحليل الشكاوي وربطها بالشكاوي الأخرى المستلمة من قبل.

---

(1) جميل عبد الباقي الصغير الجوانب الإجرائية للجرائم المتعلقة بالأنترنات،المرجع السابق. ص77.

(2)وهو إختصار لـــ: Internet Crime complaint Center

(3)وهو إختصار لـــ:Internet Fraude complaint center

(4)وهو إختصار ل National White coller center

· **قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية:** ويختص هذا القسم بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها.

· **نيابة جرائم الحاسوب والإتصالات CTC**(1) وتتألف من مجموعة من قضاة النيابة العامة ممن تلقوا تدريبات مكثفة على نظم المعالجة الآلية للبيانات وتم منحهمصلاحيات واسعة في مجال الجرائم المعلوماتية والعدوان على حقوق الملكية الفكرية.

· **المركز الوطني لحماية البنية التحتية** التابع للمباحث الفدرالية الأمريكية وقد حدد هذا المركز البنى التحتية التي تعتبر هدفا للهجومات والإعتداءات عبر الأنترنات وعلى رأسها شبكات الإتصالات.

وإضافة إلى هذه الأجهزة يوجد أيضا في الولايات المتحدة الأمريكية وحدة متخصصة بمكافحة الإجرام المعلوماتي تابعة لقسم العدالة الأمريكي تتكون من خبراء في نظام الحوسبة والأنترنات ومن مستشارين قانونيين(2).

2/في بريطانيا: قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث والتحري عن الجرائم المعلوماتية وتضم هذه الوحدة نحو ثمانين عنصرا على درجة عالية من الكفاءة في المجال التقني، وقد بدأت هذه الوحدة نشاطها عام 2001.

3/في فرنسا: قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم المعلوماتية ونذكرمن هذه الأجهزة:

· **القسم الوطني لقمع جرائم المساس بالأموال والأشخاص** ويتكون هذا القسم من محقيقين مختصين في التحقيق بجرائم العالم الإفتراضي وقد بدأ هذا القسم مهامه عام 1997.

· **المكتب المركزي لمكافحة الإجرائم المرتبط بتكنولوجيا المعلومات والإتصالات** ويعد هذا المكتبسلاح الدولة الفرنسية في مكافحة الجرائم المعلوماتية، وقد تم إنشاؤه في 2000/05/15.

---

(1)وهو إختصار لــComputer coordinattor and Télecommunication

(2) نبيلة هبة محمد هروال، الجوانب الإجرائية لجرائم الأنترنات في مرحلة جمع الإستدلالات للطبقة الأولى، دار الفكر الجامعي الإسكندرية، 2007، ص108.

4/ في الصين: قامت السلطات في هذا البلد بإنشاء وحدة متخصصة على مستوى جهاز الشرطة تعرف بإسم" القوة المضادة للهكرة" وهي تختص برقابة المعلومات التي يسمح لمواطنيها الدخول إليها عبر الأنترنات.(1)

وأما على مستوى الدول العربية فنجدها لم تقف مكتوفة الأيدي أمام خطر الجرائم المعلوماتية، فقد قامت بعض الدول منها بإنشاء أجهزة متخصصة لمكافحة هذه الجرائم ونذكر على سبيل المثال:

1/ الأجهزة المتخصصة في مصر: قامت وزارة الداخلية في مصر بإنشاء عدة أجهزة أوكلت لها مهمة ضبط ما يقع من جرائم من خلال الشبكة المعلوماتية نعرض لها على النحو التالي:

- **إدارة مكافحة جرائم الحسابات وشبكات المعلومات:** أنشئت هذه الإدارة بموجب قرار وزاري(2) وهي تابعة للإدارة العامة للمعلومات والتوثيق وتخضع للإشراف المباشر لمدير الإدارة العامة وتشرف عليها فنيا مصلحة الأمن العام التابعة لوزارة الداخلية، وتضم ثلاث أقسام رئيسية: هي قسم العمليات، قسم التأمين وقسم البحوث والمساعدات الفنية.وتعتبر هذه الإدارة من أكبر الإدارات تعاملا مع الجرائم المعلوماتية،فهي تتكون من ضباط متخصصين في مجال تكنولوجيا الحسابات والشبكات وتختص بمكافحة جرائم الأنترنات على مختلف أنواعها.(3).
- **قسم مكافحة جرائم الحاسبات وشبكات المعلومات** وقد أنشئ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة، ويتبع إدارة المعلومات والحاسب الآلي ويخضع من حيث الإشراف الفني لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات ويختص بعمليات تأمين ورقابة نظم وشبكات المعلومات لمنع وقوع أية جرائم عليها بإستخدام الأساليب والتقنيات العلمية الحديثة، ورصد ومكافحة وضبط الجرائم التي تقع بإستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات.

ثانيا:الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الوطني:أما الوضع في بلادنافإنه وبالنظر إلى الخصوصية التي تتميز بها الجريمة المعلوماتية كان الأمر محتما لتوفير كوادر

---

(1)عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنات.الطبعة الأولى.دار النهضة العربية.القاهرة2004، ص812.

(2)قرار وزير الداخلية المصري رقم 13507 لسنة 2002 الصادر بتاريخ 2002/07/07.

(3)نبيلة هبة هروال، المرجع السابق، ص141.

وأجهزة متخصصة تُعنى بعملية البحث والتحري عن الجريمة المعلوماتية وكان ذلكإما على مستوى جهاز الشرطة أو الدرك الوطني.

فعلى مستوى جهاز الشرطة فقد أنشات المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي هذه المخابر علىفروع تقنية من بينها خلية الإعلام الآلي،بالإضافةإلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة مهمتها التحقيق في الجريمة المعلوماتية تعمل بالتنسيق مع هذه المخابر.

أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية. بالاضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتيةومكافحتهاببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني وهو قيد الانشاء.

الفرع الثاني: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوىالدولي والإقليمي:

سبق وأن أسلفنا الذكر بأن الجرائم المعلوماتية تتميز بأنها عابرة للحدود الوطنية يمكن أن يتعدى أثرها عدة دول، لذلك كان لابد من وجود تعاون دولي من أجل مكافحة هذا النوع من الإجرام.ومن أساليب التعاون الدولي التعاون الأمني الذي يمكن أن يحقق أهدافه لا قبل للشرطة الإقليمية بتحقيقها، ومن أبرز هذه الأجهزة في مجال مكافحة الجرائم المعلوماتية على هذا الصعيد نذكر ما يلي:

أولا :على المستـــوى الـــدوليتعد المنظمة الدولية للشرطة الجنائية (الأنتربول)[1] من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة ومنها الجرائم المعلوماتية، وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال من أجل مكافحة الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالمعلوماتية.وتستخدم هذه المنظمة لتحقيق أهدافها وسيلتين:

([1])بعد إنتهاء الحرب العالمية الثانية عقد في بروسكل (بلجيكا) مؤتمر دولي في الفترة من 9-6/9 عام 1946 إنتهى إلى إحياء اللجنة الدولية للشرطة الجنائية (ICPO) ونقل مقرها إلى باريس وغير إسمها ليصبح المنظمة الدولية للشرطة الجنائية الأنتربول ووضع ميثاق هذه المنظمة في الفترة من 7-1956/06/13 وإعتبرنافذا إعتبارا من 1956/06/13.

الأولى: تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.

الثانية: التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

وتعمل المنظمة الدولية للشرطة الجنائية في مجال الجرائم المعلوماتية بوضع قائمة إسمية لضباط متخصصين يمكن الإستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية، كما توفر هذه المنظمة للدول الأطراف المعلومات اللازمة عن الطرق العملية في مجال الجريمة المعلوماتية من خلال خلق فرق عمل وورشات تكوين.[1] ولقد أنشأت هذه المنظمة وحدة متخصصة في مكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الإجرام وكيفية التدريب على مكافحته.

ثانيا: الأجهـــزة على المستـــوى الإقليمي:

- **الشرطة الأوروبية أو الأوروبول:** وهو جهاز على مستوى الإتحاد الأوروبي تم إنشاؤه في لكسنبورغ عام 1992 ومقره في مدينة لاهاي بهلندا ليكون حلقة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال الجرائم الإرهابية والمخدرات والجريمة المنظمة وكذا الإجرامالمعلوماتي.ويهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشرطة لمختلف الدول الأعضاء، وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة ومنها الجريمة المعلوماتية.

وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه إسم "ICROS (Internet Crime Repporting online System) في سنة 2010 بغرض التنسيق أكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الأعضاء.

- **الأوروجست:Eurojust:** وهو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، تم إنشاؤه عام 2002 وينعقد إختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الإتحاد الأوروبي أو دولة عضو مع دولة

---

[1]-Myriam QUEMENER.Cyebrcrininalité droit pénel appliqué. econonica Septembre 2010p208.

أخرى من غير الإتحاد الأوروبي.ويعد الأروجيست وحدة للتعاون القضائي، مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيقات ومباشرة متابعات جزائية.(1)

المطلب الثاني:خصائص التحقيق و المحقق في الجريمة المعلوماتية:

تعد مرحلة التحقيق الإبتدائي أو ما يطلق عليها مرحلة جمع الإستدلالات، مرحلة هامة في سبيل البحث والتحري عن الجرائم،وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة المعلوماتية، لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها. فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب إرتكاب الجريمة مباشرة قد لايبقى متاحا بعد مرور وقت قصير على إرتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم.ففي كثير من الجرائم المعلوماتية لم يترك الجاني وراؤه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والمزوجبالإحباط والإعحاب معا.(2)

الفرع الأول: خصائص التحقيق في الجريمة المعلوماتية:

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة و راسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة.

وهذه القواعد إما قانونية و إما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والإمتثال. أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته الكثير(3)

ذلك أن الفكر البشري المتعلق بالمجرم المعلوماتي يجب أن يقابله فكر بشري من قبل المحقق الجنائي، وبالتالي فإن أسلوب التحقيق وفكر المحقق الجنائي يجب أن يتغير ويتطور أيضا، وذلك كنتيجة طبيعية لمواجهة فكر المجرم المعلوماتي.

أولا: منهج أو أسلوب التحقيق الإبتدائي في الجريمة المعلوماتية:التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى إكتشاف الجريمة ومعرفة مرتكبيها تمهيدا

[1]Myrian QUEMENER.YES CHOR PENAL Cybescviminalité Droit pénal appliqué p 209.

([2]) محمد طارق عبد الروؤف الحن، المرجع السابق ص230،

([3])خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الطبعة الأولى2009.ص56.

لتقديمهم إلى المحاكمة، وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمظاهات البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي.

والهدف من التحقيق الإبتدائي هو التأكد أولا من وقوع جريمة يعاقب عليها القانون، ومن ثمة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكذا معرفة وقوعها وما هي الوسائل التي إستعملت في إرتكابها. ويكون ذلك في الجريمة المعلوماتية وفقا لمنهج تحقيقي يختلف عن غيره بالنسبة للجرائم الأخرى.

1/وضع خطة عمل التحقيق: يبدؤالمحقق عمله عند تجميع الإستدلالات المتعلقة بالجريمة المعلوماتية بوضع خطة العمل اللازمة على ضوء المعلومات المتوافرة لديه، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك على النحو الآتي:

- وضع الخطة المناسبة و التي لا تبدء إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة.
- التخطيط الفني للتحقيق وذلك من أجل الوصول إلى أفضل الطرق والأساليب للتعامل مع هذه الجرائم بالتفصيل والوضوح.
- عمل دراسة وافية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في فريق التحقيق.
- تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل وهو ما يؤدي إلى ضمان مستوى جيد من الأداء.
- تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبرة أو نقص المعرفة، وبالتالي تساعد على إيجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسيير ضمن الضوابط التشريعية وتقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة.(1)

ويجب أن ترتكز خطة العمل على مجموعة من البنود الأساسية يتم الإرتكاز عليها أثناء تنفيذ الخطة، وهي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب

(1)محمد نصير السرحاني،مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الانترنات،رسالة ماجيستار. جامعة نايف العربية للعلوم الامنيةالرياض 2004 ص72.

إستضاحها معهم وتقدير مدى الحاجة للإستعانة ببعض الفنيين اللازم توافرهم لإستكمال التحقيق،[1]بالإضافة إلى مراعاة الظروف والملابسات المحيطة بالواقعة ذلك أن من هذه الظروف ما يشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل ومنها:

- مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة.
- مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها.
- مستوى الإختراق الأمني الذي تسبب فيه الجاني.

ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش وذلك من خلال تحديد نوع الأدلة التي يريد فريق التحقيق البحث عنها.

2/تشكيل فريق التحقيق: إن التحقيق الإبتدائي في الجرائم المعلوماتية يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده، حتى ولو كانت المضبوطات هي مجرد حاسب شخصي واحد، ولذلك فإنه يفضل أن يتعاون عدة محققين في إنجاز مهمة التحقيق والعثور على الأدلة.

ويجب أن يتشكل فريق التحقيق من فنيين وأخصائيين ذوي خبرة في مجال الحاسوب والأنترنات، ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص. ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والأنترنات ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة.[2]

وإن كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا أنه يأخذ أهمية خاصة في الجرائم المعلوماتية لما تتطلبه من مهارات فنية وخبرات متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا.ومن الناحية العملية غالبا ما يتكون فريق التحقيق في الجرائم المعلوماتية من:

- المحقق الرئيسي ويكون ممن لهم خبرة في التحقيق الجنائي.
- خبراء الحاسوب وشبكات الأنترنات الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم.

([1])هشام رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط 2000، ص59.

([2])عبد الله حسين محمود، إجراءات جمع الأدلة في الجريمة المعلوماتية،مؤتمر الجوانب القانونية والامنية للعمليات الالكترونية.دبي 2003 ص612.

- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.
- خبراء التصوير والبصمات والرسم التخطيطي(1).

وفي هذا الإطار نجد أن الشرع الجزائري قد أشار إلى مسألة إمكانية إستعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية، وذلك بغرض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك(2)

ثانيا: العناصر الأساسية للتحقيق الإبتدائي في مجال الجريمة المعلوماتية: ونقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، وهناك إجراءات وإحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الإبتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الإبتدائي(3).

1/**الإجراءات التي يجب مراعاتها قبل البدء في التحقيق:** ويمكن أن نسرد الأهم منها كما يأتي:

- تحديد نوع نظام المعالجة الآلية للمعطيات فهل هو كومبيوتر معزول أم متصل بشبكة معلومات.
- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.
- إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الإتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الإختراق من عدمه، وهل هناك حواسيب آلية خارج هذه المشكلة ولها إمكانية الإتصال بها أم لا؟
- مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.

(1)عبد الله محمود، المرجع السابق، ص613.

(2)أنظر المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

(3)جميل عبد الباقي الصغير، المرجع السابق، ص119 ود. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير المعلوماتي، دار الكتب القانونية المحلة الكبرى، ط1، ص84 وكذلك د.محمد الأمين الشبري، المرجع السابق، ص50.

- مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.

- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الإستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار جريمته.

- فصل خطوط الهاتف حتى لا يسيء الجاني إستخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون إستخدامها لطمس البيانات.

- التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه من الخدع التي يستعملها الجاني عند الإختراق أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتضليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.

- إبعاد الموظفين عن أجهزة الحاسب الآلي بعد الحصول منهم على كلمة السر وكذا الشفرات في حالة وجودها.

- تصوير الأجهزة المستهدفة(التي وقعت بها أو عليها الجريمة) من الأمام والخلف وذلك لإثبات أنها كانت تعمل وكذلك للمساعدة في إعادة تركيبه من أجل البدء في إجراءات التحقيق.

2/الإجراءات التي يجب مراعاتها أثناء التحقيق: عند البدء في عملية التحقيق الإبتدائي سيما عند القيام بعملية تفتيش جهاز الحاسوب فإنه على رجال الضبطية القضائية وبرفقتهم الخبراء الذين يستعينون بهم مراعاة ما يلي:

- عمل نسخة إحتياطية من الأقراص الصلبة أو الأسطوانة المرنة قبل إستخدامها والتأكد فنيا من دقة النسخ عن طريق الأمر(disk comp).

- نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

- أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات الممسوحة، ويمكن إستعادتها من سلة المهملات مع ملاحظة أن هناك بعض الملفات التي إن مسحت وضغط على أزرار معينة مثل **Shift delete**في وقت واحد لا يمكن إستعادتها وكذا من أجل معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.

- العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد إستخدمت في جريمة إختلاس معلوماتي.

- العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.

- حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.

الفرع الثاني: خصائص المحقـــق المعلومـــاتي:

أمام التطور التقني والتكنولوجي الذي صاحب الجريمة المعلوماتية فإن المختصصين بالتحقيق فيهذا النوع من الإجرام المستحدث يختلفون عن أولائك المختصين بضبط الجرائم التقليدية من حيث الخصائص وطريقة التكوين، ذلك أن التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية وإنما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمة البحث والتحري عن الجرائم المعلوماتية وكشف النقاب عنها.

وإذا كان قد سبق وأن طرحنا خصائص الجريمة المعلوماتية وكذا خصائص المجرم المعلوماتي .فإنه في إعتقادنا يلزم الأمر معرفة الخصائص التي يجب أن يتوفر عليها من يتصدى لمهمة البحث والتحري عن هذا النوع من الجرائم والمجرمين.

أولا: الخصائص الفنية للمحقق في الجريمة المعلوماتية:تلعب الأجهزة الأمنية دورا أساسيا في صيانة أمن المجتمع وذلك إما بالقيام بدور وقائي يهدف إلى منع إرتكاب الجرائم والحيلولة دون وقوعها وتقليل فرص إقترافها، وإما القيام بدور قضائي في ضبط الجرائم ومرتكبيها بعد حدوثها.

ولقد أضاف ظهور الجرائم المعلوماتية النابعة من التطور الإلكتروني أعباء جديدة على أجهزة التحقيق لما يتطلبه التصدي لهذه الجرائم من قدرات فنية لم يألفها رجال الضبطية القضائية و لم يتعودوا عليها، ما يستلزم ضرورة توفير الإمكانات والمهارات المطلوبة في هذا المجال.

والمشكلة الأساسية التي تواجه المحققين في جرائم نظم المعلومات هي خلفية المحقق نفسه فمتخصصوا الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دوافع الجريمة وجمع الأدلة لتقديم المتهم للمحاكمة.وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول جريمة معلوماتية ما، ولكن من الناحية القانونية يتبين فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى.بينما المحققون ذوي الخلفية القانونية قد تكونلديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم[1].

([1])في حادثة طلب أحد المحققين من المشتبه فيه أن يريه الملف الذي قام بتزويره وذلك إنطلاقا من الحاسب الشخصي له فما كان للمشتبه فيه إلا أن قام عمدا بحذف هذا الملف وبذلك أضاع الدليل الرئيسي في الجريمة وفي حادثة أخرى تم القبض على بعض المتهمين وضبط الحاسوب ثم قامت

وإذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه يلزمه عند مباشرته التحقيق في الجريمة المعلوماتية معرفة العديد من الجوانب الفنية ليقوم بعمله على أحسن وجه ونذكر منها:

-معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والإنترنات والتي تتعلق بالجريمة المرتكبة ذلك أن إفتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل، على إعتبار أن جهله بأساليب إرتكاب الجريمة المعلوماتية يجعله يقع في كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة وأوعية المعلومات التي تخزن بها البيانات،[1]وبالتالي فإن الكشف عن هذه الجرائم يقتضي أن تكون الأجهزة المعنية على دراية كافية بأساسيات التعامل مع هذه الجرائم وكيفية تقصيها وضبطها وصولا إلى مرتكبيها.

- إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة، وتخزينها في الأقراص المعدة لذلك ومنع حذفها والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة أو المدمجة لأية مؤثرات خارجية كالقوى الكهرومغناطيسية أو موجات الميكروويف حتى لا تتلف محتوياتها.

- كما يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والأنترنات، وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصور كيفية إرتكاب الفعل الإجرامي في العالم الإفتراضي من إختراق للشبكات وإعتراض حزم البيانات أثناء إنتقالها عبر الشبكة والتجسس عليها وتحويلها عن مسارها، كما أنها تعطي للمحقق تصوراً جيدا عن مدى إمكانية متابعة مصدر الإعتداء على الشبكة والمعوقات التي تحول دون ذلك.[2]

جهات التحقيق بتفكيك الحاسوب بإعتباره دليل الجريمة وقامت بنقله إلى مركز الشرطة ثم بعدها تبين أن تشغيل الجهاز لفحص مكوناته يحتاج إلى إعادة توصيل الكابلات التي تم نقلها دون أن يتم ترقيمها وكان الأمر يبدو شبه مستحيل وضاع حتى الدليل أيضا.

([1])جميل عبد الباقي، الصغير. أدلة الإثبات الجنائي والتكنولوجية الحديثة،دار النهضة العربية .القاهرة2002 ص115.

([2])حسين الغافري، المرجع السابق، ص02.

- يتوجب على المحقق أن يستطيع التمييز بين الأنظمة المختلفة لتشغيل الحاسوب وأن يلم بجميع الأنظمة التشغيلية لأجهزة الحاسوب وما تتسم به من خصائص ومميزات كل نظام على حدة لأنه ملزم بالتعامل معها، وكذلك أنظمة الملفات التي يعتمدها كل نظام حتى يتمكن من إجراء التحقيق في الجرائم المعلوماتيةوفي كشف المجرمين ومعاينة مسرح الجريمة.وإذا كان التعامل المباشر مع هذه الأنظمة والقيام بفحصها ورفع الأدلة الجنائية الرقمية الموجودة فيها يعتبر مهمة الخبير" إلا أن معرفة المحقق الجنائي الأولية بهذه الأنظمة ضرورية لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة المعلوماتية.

- كما يتعين على المحقق كذلك التعرف على معطيات الحاسوب المختلفة ليصبح قادرا على معرفة صيغ الملفات وما يمكن أن تحتويه من معطيات، ومعرفته لأهم التطبيقات التي يمكنه من خلالها قراءة أو مشاهدة محتوى هذه الملفات(1) والتيتعد أمرا في غاية الأهمية، لأنها تعتبر الوعاء الحقيقي لأدلة الإدانة في كثير من القضايا ذات الصلة بالحاسوب والأنترنات بما تحتويه من معلومات.

- ومن الأمور الفنية التي يتوجب على المحقق معرفتها أيضا أن يكون ملما بالأساليب المستخدمة في إرتكاب الجرائم المعلوماتية وتقنيات الأمن المعلوماتي، ذلك أن معرفة رجال التحقيق لهذه الأساليب يعد من الأمور المهمة التي تساعدهم في معرفة الجناة ومواقع إرتكاب الجريمة ومن أي طرفية إلكترونية صدر السلوك الإجرامي وكذلك في مناقشة الشهود وسماع المشتبه فيهم ومحاصرتهم بالأسئلة التي تتعلق بكيفية إرتكاب الجريمة وطرق تنفيذها.

كما أن الإلمام بتقنيات الأمن المعلوماتية والحاسوبية من الأمور المهمة والتي لابد للمحقق المعلوماتي من معرفتها وإستعابها، لأنها تساعده في معرفة مجريات التحقيق، فالمحقق عندما يباشر التحقيق في جريمة إختراقشبكة الحاسوب التابعة لمؤسسة ما يسأل القائمين على الشبكة عن نوع برامج الحماية المستخدمة وكيفية إعدادها والكيفية التي تفاعلت بها مع الحدث محل التحقيق.وهناك الكثير من التقنيات التي تستخدم في أمن الحاسوب والشبكات والتي تكون وثيقة الصلة بالتحقيق

---

(1)يتم حفظ البيانات الرقمية داخل الحاسوب على شكل مجموعات أو كتل من البيانات تمثل وحدة واحدة تسمى الملفات ويتميز كل ملف ببينة وصيغة خاصة تميزه عن غيره، وغالبا ما ترتبط صيغة بنوع محدد من المحتوى كأن يحتوي الملف على بيانات تمثل صورا أو أصواتا أو مستندا خطيا منسق أو غير منسق.

ويكون فهم المحقق لوظائفها وأسلوب عملها وطرق إستخدامها عاملا مساعدا له عند قراءته للتقارير الجنائية التي يعدها خبير الحاسوب والتي تعد من من أهم الوثائق التي يرجع إليها المحقق ويعتمد عليها في تحقيقه و ترفق بعد ذلك بمحاضر التحقيق ويرتكز عليها توجيه الإتهام عند اللزوم.

ثانيا: تأهيل وتدريب المحقـــق المعلوماتي: في مكافحة الجرائم المعلوماتية بصفة عامة لابد من وضع سياسة جنائية رشيدة تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، ويمتد هذا التدريب والتأهيل إلى العاملين بأجهزة الضبطية القضائية.

وقد تنبهت الدول إلى هذا الأمر وظهر هذا الإهتمام في توصيات العديد من المؤتمرات الدولية الخاصة بمنع الجريمة ومعاملة المجرمين، ومنها ما جاء في القاعدة 1/22 من قواعد بيكين التي أكدت على الحاجة إلى التخصص المهني والتدريب.

ولهذا فإنه من الضروري إعداد المحققين في الجرائم المعلوماتية بإعتبارهم يواجهون أنشطة إجرامية معقدة وتنفذ بطرق دقيقة وذكية، ويتأتى ذلك من خلال الإسراع في أن يطور رجال البحث الجنائي وسائلهم البحثية وقدراتهم العلمية. وليس بالضرورة أن يكون المحقق في الجريمة المعلوماتية خبيرا في الحاسوب والنظم المعلوماتية ولكن لابد من الإلمام ببعص المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسب الآلي وحسن إستغلالهم في كشف الجرائم وجمع الأدلة كما أنه من الضروري أن يكون المحقق ملما بالإجراءات الإحتياطية التي ينبغي إتخاذها على مسرح الجريمة والتدابير اللازمة لتأمين الأدلة ومعلوماتها الممغنطة بصورة علمية وسليمة. (1)

وإذا كانت الشركات الخاصة تستعين بمحققين هم خبراء في الحواسيب، فالجهات الحكومية أولى بإعداد كوادرها للضبط والتحقيق في الجرائم المعلوماتية، فالتقدم المتواصل في تكنولوجيا الحاسب الآلي والأنترنات يفرض على جهات تطبيق القانون أن تسير في خطوات متناسقة مع التطورات السريعة التي تشهدها هذه التقنياتأ وهذا الأمر يتطلب الإلمام بالتقنيات الجديدة حتى يمكن مواجهة مجرمي المعلوماتية.

---

(1) محمد الأمين البشري. التحقيق في جرائم الحاسب الآلي بحث مقدم إلى مؤتمر القانون والكومبيوتر والأنترنات بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة الفترة من 01 إلى 03 ماي 2000.

ويرى الفقه الجنائي أنه حال التدريب على التحقيق في الجريمة المعلوماتية يتعين مراعاة عناصر أساسية تتمثل في شخص المتدربومنهج الدورة التدريبية وصفة وأسلوب التدريب.[1]

ويجب أن يشمل منهج التدريب خصوصا تدريس الأساليب الفنية المستخدمة في إرتكاب الجريمة أو الأساليب التي تتعلق بالكشف عنها وكيفية إثباتها ومعاينتها والتحفظ عليها وكيفية فحصها فنيا.

وقد كان هناك من يرى أنصعوبة التحقيق الجنائي في الجرائم المعلوماتية تتطلب أن يعهد بهذا التحقيق إلى بيوت خبرة متخصصة في هذا المجال، لكن هذا الأمر له خطورته إذ من شأنه أن يضحي بمصلحة الفرد والمجتمع ويضعها تحت رحمة هذه الشركات التي يكون همها تحقيق الربح المادي على حساب إظهار الحقيقة، فضلا عن الإخلال بمبدأ سرية التحقيق سيما لو تعلق التحقيق بجرائم عرض الأشخاص وأسرارهم الشخصية أو تعلق الأمر بأمن الدولة[2]

المطلب الثالث :الدليل المناسب لإثبات الجريمة المعلوماتي

يختلف الوسط الذي ترتكب فيه الجريمة المعلوماتية من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الإفتراضي، وعلى ضوء ذلك فان البحث في أدلة الإثبات في اطار مدى اتفاقها مع الطبيعة التقنية لهذه الجرائم ووسائل إرتكابها أصبح غير ذي معنى إذا لم يكن مدعما بتوفيق من قبل التقنية ذاتها، مما أدى الى ظهور طائفة خاصة من الأدلة الجزائية يمكن الإعتماد عليها في إثبات هذه الجرائم ومن ثمة نسبتها إلى فاعلها، بحيث تكون من ذات الطبيعة التقنية الناجمة عن النظم المعلوماتية التي تنتج عنها في حالة الإعتداء عليها وتتفق مع طبيعة الوسط الذي إرتكبت فيه الجريمة وهي الأدلة الرقميةأو الأدلة الإلكترونية حسب ما عبرت عنها الإتفاقية الأروبية لمكافحة الجرائم المعلوماتية.

فالدليل أثر يولد أو حقيقة تنبعث من الجريمة المرتكبة، ولذلك فإن طبيعة الدليل تتشكل من طبيعة الجريمة التي يولد منها. فدليل التزوير يأتي من إثبات تغيير الحقيقة في المحرر الذي يقع عليه، ودليل جريمة القتل قد يولد من فحص الأداة التي إستخدمت في القتل وطلقات الذخيرة التي

([1])هشام محمد فريد رستم، الجرائم المعلوماتية، بحث مقدم إلى مؤتمر القانون والكومبيوتر والأنترنات، ص115.

([2])محمد الأمين البشري، المرجع السابق، ص25.

إستعملت فيها. وتطبيق ذلك على الجريمة المعلوماتية فانه يمكن أن تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي إرتكبت بواسطتها أو من خلالها.(1)

وفي مجال تعامل جهات التحقيق مع الأدلة الجنائية فإن هذه الأخيرة مقبلة على الإنتقال من مرحلة التعامل مع الأدلة المادية الملموسة معروفة المصادر، إلى مرحلة التعامل مع الأدلة الرقمية المنتشرة في أماكن إفتراضية،وهو أمر لا محال يثير مشكلات مهنية وأخرى قانونية ينبغي تحديدها بوضوح توطئة لوضع الحلول المناسبة لعلاجها، ذلك أن معطيات التقنية المعلوماتية أضافت إلى مشكلة الجريمة أنماطا إجرامية على درجة عالية من التعقيد، يحتاج إثباتها إلى أسلحة وأدوات علمية نابعة من طبيعة الجريمة المعلوماتية.وسوف نحاول عرض مفهوم الدليل الرقمي ثم طبيعته من خلال ما يلي:

الفرع الأول: مفهـــوم الدليل الرقـــمي:

كما أثرت الثورة المعلوماتية على نوعية الجرائم التي صاحبتها وظهور أنماط مستحدثة من الجرائم عرفت بالجرائم المعلوماتية، فإنها في المقابل أيضا أثرت على إثباتها فأصبحت الأدلة التقليدية التي جاءت بها نصوص قانون الإجراءات الجزائية غير قادرة على إثبات هذا النوع من الجرائم الذي يحتاج إلى طرق تقنية تتناسب مع طبيعته، بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة.

أولا: تعريف الدليل الرقمي: إن تقييم أي نظام قانوني لا يمكن أن يصل إلى نتائج صحيحة إلا إذا توافر لدى المقوم تصورا واضحا لذلك النظام، وعليه فإنه من الواجب ليتسنى فهم ماهية هذا النوع من الأدلة لابد من تناول تعريفه.ولقد قبل بشأن الدليل التقني عدة تعريفات أهمها:

أنه الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها أو تحليلها بإستخدام برامج وتطبيقات تكنولوجية خاصة ويتم تقديمها في شكل دليل يمكن إعتماده أمام القضاء(2).

(1)رشيد بوكر، المرجع السابق. ص380،

(2)ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والأنترنات، دار الفكر القانونية.مصر 2006 ص88.

وهناك من يعرفه بأنه معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة النظم المعلوماتية وملحقاها وشبكات الإتصال، ويمكن إستخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة، أو جاني أو مجني عليه.(1) أو أنه الدليل الذي يجد له أساسا في العالم الإفتراضي ويقود إلى الجريمة،(2) أو أنه ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الإتصالات من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور أو أشكال أو أصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها.(3)

كما عرف الدليل الرقمي أيضا أنه مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها بإستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.(4)

وقد عرفت مجموعة العمل العلمية للأدلة الرقمية the sientific workingGrouponDigital evidenceالدليل الرقمي عام 1999 بأنه معلومات ذات قيمة إثباتية مخزنة أو منقولة في شكل ثنائي.

والتعريف الذي أخذ به التقرير الأمريكي المقدم لندوة الأنتربول العلمية حول الدليل الرقمي عام 2001،أعتبر أن الدليل الرقمي هو عبارة عن بيانات يمكن إعدادها وتراسلها وتخزينها رقميا، بحيث يمكن الحاسوب من تأدية مهام ما.

ويستخلص من التعريفات السابقة أن الدليل الرقمي، هو أي معلومات سواء كانت من صنع الإنسان أو تم إستخلاصها من الحاسوب يقبلها المنطق والعقل ويعتمدها العلم ويتم الحصول عليها

---

(1) محمد الأمين البشري مشار له لدى رشيدة بوكر، المرجع السابق .ص383.

(2) عمر محمد بن يونس مذكرات في الإثبات الجنائي عبر الأنترنات، ندوة الدليل الرقمي بجامعة الدول العربية في الفترة من 8-5 2006، ص05.

(3) الخبير عبد الناصر محمد محمودفرغلي علي ود. محمد عبيد سيف سعيد المسماري الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي الرياض في لفترة من 12-2007/11/14.

(4) طارق محمد الجملي. الدليل الرقمي في مجال الإثبات الجنائي .ورقة عمل مقدمة المؤتمر المغاربي الأول دول المعلوماتية والقانون المنعقد في الفترة من 28-10/29 2009 تنظمة أكاديمية الدراسات العليا طرابلس.بدون ترقيم.

بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب وملحقاتها وشبكات الإتصال، ويمكن إستخدامها في أي مرحلة من مراحل التحقيق أو المحكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جاني أو مجني عليه.

وبالنظر إلى جملة التعريفات السابقة، يمكن أن نلاحظ أن منها من ألحق مفهوم الدليل الرقمي بمفهوم البرنامج على الرغم من إختلافهما، فالفرق بينهما يكمن في الوظيفة التي يؤديها كل واحد منهما، فبرامج الحاسب الآلي له دور في القيام بمختلف العمليات التي يحتويها نظام المعالجة الآلية والذي لا يقوم بعمله إلا عن طريق مجموعة من البرامج تسمح بالقيام بمختلف العمليات عند إعطاء أوامر بذلك، أما الدليل الجنائي الرقمي فله أهمية كبرى ودور أساسي في معرفة كيفية حدوث جرائم الإعتداء على نظم المعالجة الآلية بهدف إثباتها ونسبتها إلى مرتكبها.

كما حصرت بعض التعريفات السابقة الأدلة الرقمية في تلك الأدلة التي يتم إستخراجها من الحاسب الآلي وهو ما يعد تضييقا لدائرة التقنية، فهي كما يمكن أن تستخلص من الحاسب الآلي فمن الممكن أيضا الحصول عليها من أي وسيلة تقنية أخرى كالهواتف النقالة الذكية.

كما ذهبت بعض التعريفات إلى إضفاء صفة الدليل الرقمي على تلك الأدلة المستخلصة من الوسط الإفتراضي، وبمفهوم المخالفة فإن تلك المعلومات التي لازالت لم يتم فصلها عن الحاسوب وهي في شكل مجالات أو نبضات مغناطيسية أو كهربائية لا تصلح لأن توصف بالدليل الرقمي وهو قول غير دقيق.[(1)].

ويرى البعض أن الأدلية الجنائية الرقمية ما هي إلا مرحلة متقدمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان، إلى الإستعانة بجميع ما يبتكره العلم من وسائل التقنية العالية ومنها الحاسوب. ولكن الحقيقة أن الأدلة الرقمية هي نوع متميز من وسائل الإثبات ولها من الخصائص العلمية والمواصفات القانونية ما يؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجنائية.

ثانيا: خصائــص الدليل الرقــمي:تقوم خصائص الدليل الرقمي على مدى إرتباطه بالبيئة التي يحيا فيها، وهي البيئة الإفتراضية والتيإنعكست على طبيعة هذا الدليل فأصبح يتصف بعدة خصائص جعلته يتميز عن الدليل الجنائي التقليدي.

([1])رشيدة بوكر، المرجع السابق. ص385.

1/الدليل الرقمي هو دليل علمي:إن الدليل الرقمي يحتاج إلى بيئته التقنية التي يتكون فيها، لكونه من طبيعة تقنية المعلومات ذات المبنى العلمي ومن ثمة فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي، فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة أن القانون مسعاه العدالة وأما العلم فمسعاه الحقيقة:. science seekstruthlaw seeks ،justice ، وإذا كان للدليل العلمي منطقه الذي يجب ألا يخرج عليه، إذ يستبعد تعارضه مع القواعد العلمية السليمة فإن الدليل الرقمي له ذات الطبيعة فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي وإلا فقد معناه.(1)

2/الدليل الرقمي من طبيعة تقنية:ان الطبيعة التقنية للدليل تقتضي أن يكون هناك توافق بين الدليل المرصود، وبين البيئة التي يعيش فيها فلا تنتج التقنية سكينا يتم به إكتشاف القاتل، أو إعترافا مكتوبا أو مالا في جريمة الروشة، أو بصمة أصبع وإنما ما تنتجه التقنية هو نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها، ومثل هذا الأمر يجعلنا نقرر أنه لا وجود للدليل الرقمي خارج بيته التقنية وأنه لكي يكون هناك دليل رقمي يجب أن يكون مستوحا أو مستنبطا من البيئة الرقمية أو التقنية(2)وهي في إطار جرائم المعلوماتية ممثلة في العالم الرقمي أو العالم الإفتراضيو هو العالم الكامن في الحاسوب والخوادم والمضيفات والشبكات التي يتم تداول الحركة فيه عبرها.

ونتيجة للطبيعة التقنية للدليل الرقمي فإنه أكتسب مميزات عن الدليل المادي من حيث قابليته للنسخ، بحيث يمكن إستخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير،(3)بالإضافة إلى إمكانية تحديد ما إذا كان الدليل الرقمي قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل بإستخدام البرامج والتطبيقات الصحيحة.

---

(1)عمر محمد أبو بكر بن يونس، المرجع السابق، ص977.

(2)خالد ممدوح إبراهيم، المرجع السابق، ص181.

(3)عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الأنترنات ندوة الدليل الرقمي، بمقر جامعة الدول العربية في الفترة من 5-2005/03/8 ص17. وقد قام المشرع البلجيكي يمقتضى القانون 2000/11/28. إلى تعديل قانون التحقيق الجنائي code instruction criminel بإضافة المادة 39 مكرر التي سمحت بضبط الأدلة الرقمية بنسخ المواد المخزنة في نظم المعالجة الآلية.

3-الدليل الرقمي دليل متنوع ومتطور: يشمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، بحيث يكون بينها وبين الجريمة رابطة من نوع خاص وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني. وتعني هذه الخاصية أنه على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة والرقمية إلا أنه مع ذلك يتخذ أشكالا مختلفة يمكن أن يظهر عليها، كأن يكون بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات والملقمات والخوادم، وقد يكون بيانات مفهومة كما لو كان وثيقة (Document) معدة بنظام المعالجة الآلية، كما من الممكن أن يكون صورة ثابتة أو متحركة (أفلام رقمية) أو معدة بنظام التسجيل السمعي البصري أو يكون مخزنا في البريد الإلكتروني، وقد يكون أيضا مرتبطا بالتشفير، وهذا التنوع إنما يعد تعبيرا عن إتساع قاعدة الدليل الرقمي بحيث يمكنه بهذه الصور أن يشمل أنواعا متعددة من البيانات الرقمية التي تصلح منفردة أو مجتمعة لان تكون دليلا بالإدانة أو البراءة.

وأما عن كون الدليل الرقمي دليلا متطورا فهي خاصية تكاد تكون تلقائية، نظرا لإرتباطه بالطبيعة التي تتمتع بها حركة الإتصال عبر الأنترنات والعالم الإفتراضي الذان لا يزالان في بداياتهما و لم يصلا بعد إلى منتهاهما ولن يكون من السهل إحتواؤهما.

4-الدليل الرقمي صعب التخلص منه: إن القاعدة التي تسري على كافة ما يتعلق بهيكلة تكنولوجيا المعلومات، هي أنه كلما حدث إتصال بتكنولوجيا المعلومات في معنى إدخال بيانات إلى ذلك العالم (Input) فإنه من الصعب التخلص منها ولو كان ذلك بإستخدام أعتى أدوات الإلغاء، فمحاولة التخلص من الدليل الرقمي بإستخدام خصائص التخلص من الملفات في الحاسوب كخاصية (Erase. Remove.Delete...)لا تعد من العوائق التي تحول دون إسترجاع الملفات المذكورة إذ تتوافر برمجيات[1]ذات الطبيعة الرقمية يمكن بمقتضاها إسترداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب.[2].

(1)مثل photorec/ recover jpeg/.foremost تستخدم لإسترجاع الصور والملفات المحذوفة من الهاردوذواكر USB

(2)عمر محمد أبو بكر بن يونس، المرجع السابق، ص982.

ويمكن اعتبار هذه الخاصية ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة التقليدية، إذ يمكن التخلص بسهولة من الأوراق[1]والأشرطة المسجلة إذا حملت في طياتها دليل الجريمة بتمزيقها أو حرقها، كما يمكن أيضا التخلص من بصمات الأصابع بمسحها عن موضعها، كما يمكن التخلص من الشهود بتهديدهم أو قتلهم كما يحدث في بعض الدول الغربية أو إستبعادها أصلا في الإثبات إذا مضى عليها مدة طويلة من الزمن قد لا يكون بعدها الشاهد قادرا على التذكر وكل ذلك يجعل عملية التخلص من هذه الأدلة أمرا سهلا، ومن إمكانية إسترجاعها أو إسترداد الدليل المستمد منها أمرا مستحيلا بعد تدميرها، أما بالنسبة للأدلة الرقمية فإن الحال غير ذلك، حيث يمكن إسترجاعها بعد محوها وإصلاحها بعد إتلافها وإظهارها بعد إحفائها، مما يؤدي إلى صعوبة الخلاص منها. كما أن نشاط الجاني في عملية محو الدليل يشكل في حد ذاته دليلا ضد الجاني لأن هذا النشاط(فعل الجاني لمحو الدليل) يتم تسجيله في الحاسب الآلي، ويمكن إستخلاصه لاحقاويترتب على هذه الخاصية مسائل قانونية هامة أبرزها مسألة التخلص أو إخفاء الدليل، وهو يعد فعلا آخر موضوع تجريم بمقتضى القانون، فإذا ثبت أن مرتكب الجريمة المعلوماتية قد إستخدم من البرمجيات من أجل التخلص من الدليل فإنه يمكن متابعته وإدانته بالنصوص القانونية التي تجرم مثل هذه الأفعال.

5-الدليل الرقمي ذو طبيعة رقمية ثنائية(1-0):إن الآثار التي يتركها مستخدم النظام المعلوماتي والتي تشمل الرسائل المرسلة منه أو التي إستقبلها وكافة الإتصالات التي تمت من خلال الحاسب الآلي وشبكة الإتصالات تكون على الشكل الرقمي، فالبيانات الموجودة داخل الحاسب الآلي سواء كانت في شكل نصوص أم حروف أو أرقام أم صور أم فيديو تتحول إلى صيغة رقمية، حيث ترتكز تكنولوجيا المعلوماتية الحديثة على تقنية الترقيم التي تعني ترجمة أو تحويل أي مستند إلى نظام ثنائي في تمثيل الأعداد يفهمه الحاسب الآلي، قوامه الرقمان (0).(1)فأي شيء في العالم

([1])ولقد كانت قضية ايران كونترا(Iran-contra)سنة 1986 من أولى القضايا التي أبرزت هذه الطبعة للدليل الرقمي وما يمتع به من صلابة ففي هذه القضية أدرك المسؤولون الأمريكيون عدم وجود إتزان في مقارنة الدليل الورقي بالدليل الرقمي فالدليل الورقي يمكن التخلص منه بتمزيق الورقة التي تحمله في حين أن الدليل الرقمي يمكن إعادته إلى الحياة حتى وإن كان قد تعرض للإزالة ففي هذه القضية أثناء التحقيق مع الكولونيل" أوليفرنورد" تم إستعادة جميع الرسائل الإلكترونية المتعلقة بالجريمة بعد أن قام هذا الكولونيل بحذفها من حاسوبه إذا لم يكن يعلم هذا الأخير أن هذه الرسائل يمكن إستعادتها عن طريق النسخ المحفوظة في النظام.

الرقمي يتكون من الصفر والواحد، [1] فالكتابة مثلا في العالم الرقمي ليس لها الوجود المادي الذي نعرفه وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد وهو الرقم الثنائي(0)(1) وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة.[2]

إن هذه الخصائص السالف ذكرها أكسبت الدليل الرقمي طابعا متميزا جعلت منه الدليل الأفضل لإثبات الجرائم المعلوماتية لأنه من طبيعة الوسط الذي إرتكبت فيه، سواء كانت هذه الجرائم مرتكبة بواسطة نظام المعالجة الآلية أو كانت تشكل إعتداء ومساسا على نظام المعالجة الآلية.

الفرع الثاني: أشكال الدليل الرقمي وأنواعه:

يقسم الدليل الرقمي إلى دليلين هما: الدليل الرقمي الأصلي وهو البنود العينية أو الحسية وكذلك المستمسكات البيانية التي تتعلق بهذه البنود عند الإمساك بها وحجزها. والدليل الرقمي المكرر وهو إستنساخ رقمي دقيق لجميع المستمسكات البيانية التي يتحتويها البند العيني الأصلي، أما المحرر الرقمي فهو بيانات يدخلها المزود ويرسلها عن طريق وسيط إلكتروني فيترجمها الوسيط وفق برنامج معين ويمررها إلى المتلقي الذي يمكنه إستخراجها بالإستعانة بوسيط إلكتروني آخر ويمكنه قراءتها بذات البرنامج وإظهارها على صورة الإدخال، وأما الصورة المأخوذة عن الدليل الرقمي فهي صورة دقيقة وطبق الأصل للمعلومات الواردة في الوثائق البيانية والمستقلة عن البنود العينية الأصلية[3]

وفي كلا التقسيمين أي سواء كان الدليل الرقمي أصليا أم مكررا فهو من حيث هيأته يوجد على عدة أشكال وصور:

أولا:أشكال الدليل الرقمي: ليس للدليل الرقمي صورة واحدة بل يوجد له العديد من الصور والأشكال:

([1])ممدوح عبد الحميد عبد المطلب، إستخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكومبيوتر،بحث منشور على الموقع الإلكتروني www.arablaw.info.com. ص08.

([2])عمر محمد أبو بكر بن يونس، المرجع السابق، ص791.

([3])عادل عزام سقف الحيط، المرجع السابق، ص233.

1/الصورة الرقمية: وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة في شكل ورقي أو في شكل مرئي بإستخدام الشاشة المرئية، والصورة الرقمية تمثل تكنولوجيا بديلة للصورة التقليدية.[1]

[1]ممدوح عبد الحميد عبد المطلب، أدلة الصورة الرقمية في الجرائم عبر الكومبيوتر. مركز شرطة دبي 2005، ص10.

2-**التسجيلات الصوتية:** وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الأنترنات.

3-**النصوص المكتوبة:** وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية ومنها الرسائل عبر البريد الإلكتروني والبيانات المسجلة بأجهزة الحاسب الآلي.

ووفقا لما قررته وزراة العدل الأمريكية سنة 2002 فإن الدليل الرقمي يمكن أن يأخذ الأشكال التالية: (1)

- السجلات المحفوظة في الحاسوب وهي الوثائق المكتوبة والمحفوظة مثل البريد الإلكتروني وملفات برامج معالجة الكلمات ورسال غرف المحادثة على الأنترنات.

- السجلات التي تم إنشاؤها بواسطة الحاسوب وتعتبر مخرجات برامج الحاسوب وبالتالي لم يلمسها الإنسان مثل"logfiles

- السجلات التي جزء منها تم حفظه بالإدخال، وجزء آخر تم إنشاؤه بواسطة الحاسوب بعد معالجتها من خلال برامج معينة.

- كما أن هناك (2)من يقسم أشكال الدليل الرقمي تقسيما يتطابق مع تقسيم الجريمة عبر الحاسب الآلي على النحو التالي:

- أدلة رقمية خاصة بأجهزة الحاسب الآلي وشبكاتها.

- أدلة رقمية خاصة بالشبكة العالمية للمعلومات.

- أدلة رقمية خاصة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

بالإضافة إلى هذا التقسيم فإنه يوجد من الفقه من إعتمد في تحديد أشكال الدليل الرقمي على أشكال المخرجات الكومبيوترية(3)إذ يأخذ الدليل الرقمي بحسب هذا التقسيم ثلاث أشكال:

- مخرجات ذات طبيعة ورقية يسجل فيها المعلومات على الورق ويستخدم في ذلك الطابعات.

- مخرجات ذات طبيعة إلكترونية تستخدم في تخزين المعلومات بدل الوثائق الورقية كالأشرطة المغناطيسية .

---

(1)سلطان محيا الريحاني، الجرائم المعلوماتية.بحث منشور على الموقع الإلكتروني. http//.www.atslp.com .بدون ترقيم

(2)ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي. المرجع السابق، ص88.

(3)تعتبر المخرجات أو كما تسمى أيضا الوثيقة المعلوماتية: أنها كل جسم منفصل أو يمكن الأنترنت فصله عن نظام المعالجة الآلية للمعطيات وقد سجلت عليه معلومة معينة سواء أكان معدا للإستخدام بواسطة نظام المعالجة الآلية للمعلومات أم يكون مشتقا من هذا النوع.

- مخرجات مرئية معروضة بواسطة شاشات الحاسب الآلي ذاته ويتمثل هذا الشكل في عرض البيانات المعالجة آليا بواسطة الحاسب الآلي على الشاشة الخاصة به.

ثانيا:أنواع الدليل الرقمي:يأخذ الدليل الرقمي نوعين رئيسيين:

أدلة أعدت لتكون وسيلة إثبات وأدلة لم تعد لتكون وسيلة إثبات، فأما النوع الأول فيمكن إجماله فيما يلي:

1- السجلات التي تم إنشاؤها بواسطة الجهاز تلقائيا، وتعتبر هذه السجلات من مخرجات الجهاز و لم يساهم الإنسان في إنشائها.

2- السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الجهاز، ومن أمثلة ذلك البيانات التي تم إدخالها إلى الأدلة وتتم معالجتها من خلال برنامج خاص. وأما النوع الثاني أي الأدلة الرقمية التي لم تعد لتكون وسيلة إثبات فهي تلك الأدلة التي تنشأ دون إرادة الشخص بمعنى أنها أي أثر يتركه دون أن يكون راغبا في وجودها، ويسمى هذا النوع من الأدلة بالبصمة الرقمية أو الآثار المعلوماتية للرقمية(1)وهي تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الإتصالات التي تمت من خلال النظام المعلوماتي وشبكة الإتصالات، والواقع أن هذا النوع من الأدلة لم يعد أساسا للحفظ من طرف من صدر عنه غير أن الوسائل التقنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوئها فالإتصالات التي عبر المنظومة المعلوماتية المرتبطة بشبكة الإتصالات وكذا المراسلات الصادر عن الشخص أو التي يتلقاها يمكن ضبطها بواسطة تقنية خاصة بذلك(2)

وتبدو أهمية التمييز بين هذين النوعين في كون أن النوع الأول من الأدلة الرقمية قد أعد سلفا كوسيلة لإثبات بعض الوقائع التي يتضمنها،لذلك فإن عادة ما يعمد إلى حفظه للإحتجاج به لاحقا وهو ما يقلل من إمكانية فقدانه كما يكون من السهل الحصول عليه، بينما النوع الثاني من الأدلة الرقمية فلكونه لم يعد أصلا ليكون أثرا لمن صدر عنه لذا فهو في الغالب ما يتضمن

(1)ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص22-38.

(2)يتم الإعتماد في ضبط هذا النوع من الأدلة على ما يعرف ببروتوكول"IP" والذي يمكن من خلاله ضبط تحركات مستخدم الأنترنات عبر الجهاز الذي يستعمله من خلال بيانات هذا الجهاز عند مزود الخدمة وإن كان هذا النظام لا يحدد شخصية مرتكب الجريمة فإنه يحدد الجهاز الذي إستعملت منه، ويرى البعض أن ذلك يصح لأن يكون قرينة على إعتبار صاحب الجهاز هو مرتكب الجريمة إلى أن يثبت العكس.

معلومات تفيد في الكشف عن الجريمة ومرتكبها ويكون الحصول عليه بإتباع تقنيات خاصة لا تخلو من الصعوبة والتعقيد، وهو على العكس من النوع الأول إذ لم يعد ليحفظ مما يجعله عرضة للفقدان بسهولة(1).

ويلاحظ أن هذا التنوع في الدليل الرقمي يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه وإنما تتعدد هذه الوسائل أيضا، ويضل في كل الأحوال الدليل المستمد بواسطتها رقميا.

المطلب الرابع: مصادر الحصول على الدليل الرقمي:

إن مصادر الحصول على الدليل الرقمي تكمن في البيئة الرقمية التي إرتكبت فيها الجريمة المعلوماتية، وتتمثل في أجهزة الحواسيب الخاصة بالجاني أو المجني عليه وكذا أجهزة مقدم الخدمة.

وهذه المصادر قد تكون على سبيل المثال لا الحصر إذ أن التطور العلمي والتقني قد يسفر عن أنواع جديدة من المصادر التقنية ، إذ المقصود هنا من أين يمكن لجهات التحقيق والتحري عن الجريمة المعلوماتية إستخلاص الدليل الرقمي.

الفرع الأول: فحص جهاز الحاسوب الخاص بالجاني و المجني عليه:

إن فحص جهاز الحاسوب الخاص بالجاني يمكن من التحقق وبيان الطريقة التي قام بها هذا الاخير في إرتكاب جرائمه، ومما لا شك فيه أن المجني عليه هو المصدر الكاشف والنتيجة التي يترتب عليها ما قام به الجاني من جرائم، وبالتالي فإن فحص جهاز الحاسوب الخاص به يمكن المحقق من معرفة الدخول وتتبع مصدره.

ويمكن الوصول إلى الدليل الرقمي المتعلق بالجرائم المعلوماتية من خلال أجهزة الحاسوب سواء الخاصة بالجاني أو المجني عليه عن طريق البحث في المصدرين التاليين:

أولا: أنظمة الحاسوب وملحقاتها:تعد الحواسيب مصدرا غنيا بالأدلة الرقمية خاصة تلك الحواسيب الشخصية التي تعد بماثبة أرشفة سلوكية للأفراد، فهذه الحواسيب تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد ورغباتهم، وعملية حجز الحاسوب بقصد تفحصه تعد نقطة البداية في الكشف عن خفايا الجريمة المعلوماتية بإعتبار أن هذا الجهاز هو وسيلة تنفيذها.والحاسب

(1)طارق محمد الجملي، الدليل الرقمي في الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة 28-2009/10/29.المرجع السابق.

الآلي في ذاته يقوم في تركيبته على أمرين هما: القطع الصلبة(Hardware) والقطع المرنة أو البرمجيات(Soft Ware) وهناك عنصر ثالث يتوزع بين البرمجيات والقطع الصلبة وهو عنصر المعلوماتية.[1]لذلك فإن الأمر يستلزم أن يكون الفحص ماديا ومعنويا للإرتباط القائم بشكل طبيعي بين مكونات الحاسوب ككل.

وقد تعتمد عملية الفحص على الحاسوب ذاته أي ما يسمى بالفحص الذاتي من خلال قيام الحاسوب ذاته بفحص مكوناته وتقديم تقرير كامل بذلك إلى طالب الفحص، ومثل هذه العملية تتطلب من القائم بها مهارة عالية أو قد يتم الفحص عن طريق الإستعانة بجهاز آخر أو أجهزة تقنية للبحث في جزئيات عبر جهاز الحاسوب.ويجب أن تشمل عملية الفحص على مايلي:

1/فحص القرص الصلب: يحتوي القرص الصلب بداخله على مجموع البيانات الرقمية ذات الطابع الثنائي والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي (0.1)، وتتم عملية فحص القرص الصلب أما كليا أو جزئيا، فالفحص الجزئي يؤدي إلى التعرف على محتوى البياناتوالتي يؤدي التعامل معها إلى الكشف عن القيمة الإستردادية للبيانات المخزونة فيه سواء كانت محتويات مكتوبة، صور أو أصوات......إلخ.

بالإضافة إلى إمكانية معرفة ما تم حذفه من بيانات وبرامج بالإستعانة ببرمجيات خاصة للقيام بذلك،[2]والمثال المستخدم هنا هو حالة البحث في ملفات النسخ وهذه الأخيرة هي عبارة عن ملفات تأخذ نسخة إحتياطية عن كل صفحة يتم الولوج إليها عبر الأنترنات كما توجد ملفات خاصة بالتنـــزيل(Download file) مهمتها إستقبال الملفات التي يتم تحميلها على جهاز الحاسب الآلي من خارجه وعبر الأنترنات فهذه الملفات مركزها القرص الصلب.

وللتعرف على محتويات القرص الصلب فإن ذلك يتوقف على مسائل عديدة منها الكيفية التي يتم بها ضبط الحاسوب ومهارة الشخص القائم بإستخلاص البيانات دون العبث بمحتوياتها لذلك فإنه عند ضبط جهاز الحاسب الآلي، على المحقق أن ينتزع القرص من الجهاز الخاص به ويحافظ عليه من الإرتجاج أو الإصطدام بأي شيء، وعدم محاولة تفريغ أي بيانات متواجدة عليه

---

(1)حسين بن سعيدبن سيف الفاغري، المرجع السابق، ص425.

(2)عمر أبو بكر بن يونس، المرجع السابق، ص10-11.

وذلك تلافيا لفقد أي بيانات، وتسليمه إلى الفني الخبير المختص الذي يقوم بتحليل النسخ التي تصدر من القرص وبعرض ما توصل إليه على المحقق.

وهنا لابد من مراعاة شرط سلامة جهاز الحاسب الآلي، الذي يعني صحة حركة القطع الصلبة فيه وذلك لتجنب الوقوع في مأزق رفض المحكمة الإعتداد بالدليل المنبثق عنه، فشرط سلامة الحاسوب مطعن رئيسي على كل دليل تم الحصول عليه بحيث يجب الكشف على حركة الحاسوب بداية والإقرار بسلامته.(1)

وإن من الأشياء التي تظهر بعد عملية فحص أي قرص صلب لأي جهاز تلك البيانات التي كان يستخدمها الجاني، وكذا الصور المخزنة فيه ومخابئ صفحات الأنترنات، ومن خلالها يمكن التوصل لصفحات وعناوين مواقع الأنترنات وكذا رسائل البريد الإلكتروني بالإضافة إلى رؤوس الصفحات المرسلة والمتلقاة ومجموعة البرامج الجاهزة المتخصصة التي إستخدمها (المشتبه فيه) ومنها يمكن تحديد أصدقاء (المشتبه فيه) وكذا تحديد ما يتحاورون فيه.

2/فحص البرمجيات: يتطلب الأمر في مثل هذه الحالة أن نميز بين الفحص الداخلي للبرمجيات والفحص الخارجي لها. فالفحص الداخلي يتم من خلال البحث في البناء المنطقي للبرمجة بما يوحي بأن هناك مجهودا تجديديا في إعداده للعمل حين إنزاله على جهاز الحاسب الآلي Instalationمن خلال تتبع خطوات منطقية تعبر عن هذا الجهد، وأكثر ما يتم البحث عنه في إطار الفحص الداخلي هو البحث عن مصدر الملفات الموجودة في هذا الإطار، ذلك أن النسخ عبر الأنترنات لا يشبه النسخ بإستخدام برمجيات المعالجة فالأول نسخ عبر العالم الإفتراضي والثاني يتم بإستخدام مصنف متداول في العالم المادي.وتفيد وسيلة النسخ في ترتيب كيفية حدوث الجريمة.

أما في حالة الفحص الخارجي والذي يتم اللجوء فيه إلى النسخة الأصلية للمقارنة بينها وبين النسخة محل الإشتباه وذلك للدلالة على ثبوت إرتكاب الجريمة بدرجة مقنعة.

وفي كلتا الحالتين ينبغي التنبيه إلى خطورة البرمجيات المعيبة التي يمكن أن تؤثر في الحاسوب وتجعله محل شك تهتز معه قيمة الدليل، يكون لهذا القصور أثره في عملية تقييم الدليل المستمد من البرمجيات ذاتها(2)

---

(1)خالد ممدوح إبراهيم .الجرائم المعلوماتية، المرجع السابق.ص215.

(2)خالد ممدوح إبراهيم، المرجع السابق، ص219.

3-فحص النظام المعلوماتي: إن المهمة الأساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر التي يمكن أن يقوم بها مستخدم الحاسوب، وتعني عملية فحص النظام المعلوماتي ضبط كافة ما يحتويه جهاز الحاسب الآلي من معلومات [1]يمكن إسترجاعها عبره تكون مخزنة في ملفات على أي شاكلة يمكن أن تكون عليها الحركة الإستردادية ما دام موضوعها يشكل جريمة.

والحقيقة أنه على حسب كثرة التعامل بالحاسب الآلي يتكاثر محتوى النظام المعلوماتي مما يزيد من صعوبة فحصه بالنظر إلى الحجم الضخم والكم الهائل من المعلومات المخزنة فيه.

بالإضافة إلى أن عملية تخزين البيانات لا تتخذ شكلا محددا وإنما تتنوع أساليبها، والتي يصل مداها إلى حد إمكانية تخزين البيانات بشكل آمن في الحاسوب بنظام التشغيل أو بنظام إخفاء البيانات المعلوماتي بحيث لا يظهر الملف حتى في حالة البحث الآلي للحاسب عنه والذي قد يحتوي على مواد إجرامية، وتفوت الفرصة بسبب هذه التقنية على المحققين من الوصول إليه.[2]

ثانيا: فحص أنظمة الإتصال بالأنترنات: يقصد بنظام الإتصال بالأنترنات بالمفهوم الإجرائي هو تلك الأجراءات أو المراحل المتبعة حال إستخدام الإتصال بالأنترنات، ومن أهم المسائل المثارة في صدد فحص أنظمة الإتصال بالأنترنات سعيا وراء البحث عن الدليل هي مسألة تحديد مكان الجريمة أو جهاز الحاسب الآلي الذي إنطلق منه النشاط الإجرامي، وذلك من خلال تتبع الحركة العكسية لمسار الأنترنات أي تتبع الحركة التراسلية للنشاط الممارس من خلال الأنترنات، فالحاسوب بمجرد أن يتعرف على المسار يقوم تلقائيا بإختيار البروتوكول التراسلي الذي من خلاله يقوم بإستدعاء البيانات.[3]

([1])إن النظام المعلوماتي للحاسب الآلي لا يحتوي على معلومات مكتوبة كما هو المعتقد السائد، وإنما المحتوى المعلوماتي عادة ما يتكون من بيانات ثنائية الهيئة الرقمية يتم إيداعها في الحاسب الآلي في شكل تخزين (Stockage) ويقوم الحاسوب بمعالجة هذه البيانات ويبرزها على هيأة معلومة محددة حين يتم إستدعاؤها من قبل مستخدم الحاسوب وما دام لم يتم إستدعاء معلوماة محددة فإن بياناتها تضل في حالة تخزين في الحاسوب فلا يقوم الحاسوب بإستدعاء كافة المعلومات مرة واحدة.

([2])خالد ممدوح إبراهيم، المرجع السابق. ص222.

([3])عمر بن يونس الجرائم الناشئة عن إستخدام الأنترنات،المرجع السابق. ص998.

ويستخدم في عملية تتبع حركة مسار الأنترنات نظام فحص إلكتروني يطلق عليه علم البصمات المعاصر،[1]وما يتم التوصل إليه بعد ذلك هو عنوانرقمي يسمى adresse IPInternet protocolو هو عبارة عن برتوكول لعنونة البيانات والمواقع في شبكة الأنترنات، وبمقتضى هذا البروتوكول(IP) يتم التعرف على الكومبيوتر الموصول بشبكة الأنترنات من خلال عناوين عددية، حيث لكل كومبيوتر بها عنوانه الوحيد والخاص به تماما[2]يسمىIPAdresseوكل عنوان IPمكون من جزئين الأول يشمل أرقام الشبكة والثاني يشمل أرقام مقدم الخدمة[3]ويعمل بروتوكول IPبشكل متزامن مع بروتكول آخر وهو بروتوكول التحكم بالنقل (Trams mission control TCP(protocolوهذان البرتوكولانTCP/IPهما من عائلة برتوكولات الإتصال بين عدة أجهزة من الحواسيب طورت أساسا لنقل البيانات بين أنظمة(UNIX) [4]ثم أصبحت المقياس المستخدم لنقل البيانات الرقمية عبر شبكة الأنترنات، ويرتكز البرتوكولان معا (TCP/IP) على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Pachet) بين مختلف الوصلات السلكية واللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصولة فيما بينها. وحزمة المعلومات جزء أو قسم من ملف معلوماتي ذات حجم مصغر ثابت تحمل كل منها رقما خاصا ومعلومات تعريفية بكل من المرسل والمرسل إليه، وعند كل وصلة تتم قراءة جهة المقصد أو المرسل إليه ثم تتم إعادة إرسال الحزمة المارة عبرهما نحو الوصلات التالية الأقرب إلى جهة المقصد النهائية.

([1])وقد تم إستخدام هذا المنهج في الكشف عن العديد من الجرائم مثل تتبع مبتكر فيروس ميليسا وكذا التوصل إلى الشخص الذي إبتكر موقع خدمات بولمبروج لأخبار المال الإحتيالي لكن يرفع الأسهم بطريق الخداع.

([2])عبد الحميد عبد المطلب إستخدام برتوكول TCP/IP في بحث وتحقيق الجرائم مع الكومبيوتر، المرجع السابق.ص5.

([3])يعبر عن عناوين الأنترنات الرقمية الوحيد سلسلة مؤلفة من أربع مجموعات من الأرقام مفصولة عن بعضها بنقاط أو حروف أبجدية رمزية دالة عليها، يجري صفها ضمن تسلسل هرمي ويتولى نسخ هذه الأرقام أو إستبدالها بحروف مؤسسة الأنترنات لمنح الأسماء والأرقام وهي لجنة دولية خاصة تعمل بالتنسيق مع المنظمة الدولية للملكية الفكرية مهمتها إبتكار آلية لمنح عناوين المواقع وتأخذ في الحسبان البعد الدولي لشبكة الأنترنات وكيفية حل المنازعات بشأنها، وكان يقوم بهذه المهمة قبل إنشاء المؤسسة عام 1988 لجنة منح الأرقام في الأنترنات وهي هيئة أناطت مؤسسة الأنترنت بها مهمة إدراة نظام منح عناوين الأنترنات حسب برتوكول IP قبل أن تنتقل هذه المهمة إلى مؤسسة الأنترنات لمنح الأرقام والأسماء.

([4])UNIX هو نظام تشغيل متعدد المهام ومتعدد المستخدمين مصمم لإستخدامه في الكومبيوتر المنزلي أو المكتبي بإعتبار أن هذا النظام مكتوب بلغة (C) لذلك فهو أكثر قابلية للنقل المعلوماتي من الأنظمة الأخرى، واللغة (C) لغة برمجة عالية المستوى صممت أصلا لتعمل تحت النظام UNIX وهي مستخدمة في كتابة كافة التطبيقات بعد أن يرى وضع مقاييسها من قبل المعهد القومي الأمريكي للمقاييس.

ويعتبر نظام TCP/IP من أكثر البرتوكولات المستخدمة في شبكة الأنترنات فهو جزء أساسي منه، لذلك تبرز أهمية الإستعانة بالمعلومات والمصادر والعناوين التي يمكن أن يحتويها هذا البرتوكول في تحقيق الجرائم المعلوماتية، حيث تدل بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة وتحديد الأجهزة التي أصابها الضرر من الفعل الأجرامي وتحديد نوعية النشاط الإجرامي من خلال الفترة الزمنية لإقتراف الجريمة(1).

ويتنازع إمكانية تحديد مسار الأنترنات من عدمه رأيان، إذ يذهب رأي إلى أنه لا يمكن تحديد مسار إرتكاب الجريمة وتكمن وجاهة هذا الرأي في أن شبكة الأنترنات ذات طبيعة مرنة بحيث أنه حتى وإن أمكن مستقبلا تحديد مسار الأنترنات، فإن ما يتم الحصول عليه في هذا الإطار إنما هو دليل رقمي يحتاج إلى تكملته بأدلة إثبات أخرى، فيما لو إقتصر الأمر على هذا الدليل فإن الأمر يظل في حومة الشك(2)ذلك أن ما يتم التوصل إليه في الحقيقة من خلال الدليل الرقمي إنما هو عنوان رقمي فقط (adresse TP) وهذا لا يكفي في نسبة العمل الإجرامي إلى صاحب الحاسوب أو العنوان المذكور، إذ من الممكن ألا يكون هو مرتكب الجريمة كما لو كان جهاز الحاسوب مسروقا أو يكون أحد يستخدمه إحتيالا أو يتم إستخدام جهاز الحاسوب في مقهى الأنترنات، فمثل هذه الأمور تجعل من الصعوبة بمكان الإعتماد على مسار حركة الأنترنات للتوصل إلى تحديد شخص الجاني وإنما قد يحتاج الأمر إلى دليل مادي مكمل للدليل الرقمي، ويمكن التأكيد على أنه حتى في الحالات التي تمت فيها إدانة أشخاص أمام القضاء المقارن كان هناك دائما دليل مادي يتم الإستناد إليه إلى جوار الدليل الرقمي. في حين يذهب الرأي الآخر إلى القول بإمكانية تتبع مسار الأنترنات ويمكن من خلال هذا التتبع التوصل إلى تحديد مسار العمل الإجرامي.

وتجدر الإشارة إلى أنه في إطار فحص نظام الإتصال بالأنترنات كمصدر يمكن من خلاله البحث عن الدليل الرقمي، يتضمن أيضا لزوم فحص الخادم أو الملقم "serveur"وهو حاسوب ضخم مهمته تحقيق حركة الإتصال بالمواقع والصفحات التي تتم إستضافتها على هيئة رقمية فيه، لذلك فإنه يطلق على الخادم lieu de stokage numerisees des donnees

(1)ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص1.

(2)خالد ممدوح إبراهيم، المرجع السابق. ص207-208

الفرع الثاني: تعاون مزودي الخدمة مع جهات التحقيق:

لما كان الدليل الرقمي قابع في البيئة التقنية ويتسم بخصائصها، وهي خصائص تبنى على أساس الطبيعة المرنة التي عليها العالم الإفتراضي، فإن للفاعل إمكانية إزالة الدليل من على بعد بإستخدام التقنية ذاتها. من أجل ذلك إستلزم الأمر وضع إطار قانوني وهو نظام إلزام مزودي الخدمة(1) بحفظ المعطيات.

وهذا ما تضمنه قرار الجمعية العامة للأمم المتحدة رقم (63/55) المؤرخ في 2001/01/22 والمتعلق بمكافحة إساءة إستعمال تكنولوجيا المعلومات لأغراض إجرامية، وذلك في الفقرة "و" من المادة الأولى منه والتي ألزمت الدول أن تسمح بحفظ المعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية الخاصة وسرعة الوصول إليها وهو ما أكده المشرع الجزائري بموجب المادة 10 من الفصل الرابع في القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها تحت عنوان "إلتزامات مقدمي الخدمات."

أولا: المقصود بمزودي الخدمات: حسب المادة الأولى فقرة"ج" من إتفاقية بودابست فإن مزود الخدمة هو كل من يقوم بخدمات الإيصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، وقد يكون جهة عامة أو جهة خاصة وقد يقدم خدماته للجمهور أو لمجموعة من المستخدمين الذين يشكلون مجموعة مغلقة.

ويعرف قانون حماية الحياة الخاصة في مجال الإتصالات الإلكترونية في الولايات المتحدة الأمريكية نوعين من مزودي الخدمة:

النوع الأول: مزود خدمة الإتصالات الإلكترونية ويقصد به كل من يقدم خدمة إلى مستخدمي الشبكة والتي تتمثل في تسهيل إرسال وإستقبال الإتصالات الإلكترونية.

والنوع الثاني وهو مزود خدمة الحوسبة عن بعد ويقصد به كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بوسيلة من وسائل الإتصالات الإلكترونية.

---

(1)أورد المشرع الجزائري في المادة 10 أنه في إطار تطبيق أحكام هذا القانون (04/09) يتعين على مزودي الخدمة تقديم المساعدات للسلطات المكلفة بالتحريات القضائية... بوضع المعطيات التي يتعين عليهم حفظها وفقا لأحكام المادة 11 أدناه تحت تصرف هذه السلطات.

وقد عرف المشرع الجزائري موزد الخدمة (مقدم الخدمة) بموجب الفقرة 06 من المادة الثانية في القانون 04/09 بأنه:

1/كل كيان عام أو خاص يقدم لمستعملي خدماته ضمانة القدرة على الإتصال بواسطة منظومة معلوماتية و/أو نظام للإتصالات.

2/ أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الإتصال المذكورة أو لمستعمليها.

وعلى هدي ذلك فإن المراسلة بالبريد الإلكتروني والتي يتم إستقبالها بواسطة مزود الخدمة الخاص بالمرسل إليه والتي لم يطلع عليها بعد،فإنها تستقر في حالة تخزين إلكتروني وتكون في هذه المرحلة النسخة من الإتصال المخزنة تتواجد فقط كإجراء أو وسيط مؤقت في إنتظار إستقبال المرسل إليه لها من مزودالخدمة، وبمجرد إستلام المرسل إليه المراسلة بالبريد الإلكتروني فإن الإتصال يكون قد وصل إلى وجهته الأخيرة، وهنا يكون موقف مزود الخدمة يتراوح بين أمرين: إما أن يقوم بمسح تلك الرسالة أو يقوم بالإحتفاظ بها.(1)

ثانيا إلتزامات مقدمي الخدمة: ألزم المشرع الجزائري مقدمي الخدمات بحفظ المعطيات،(2)وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازتها في أرشيف ووضعها في ترتيب معين في إنتظار إتخاذ إجراءات قانونية محتملة أخرى كالتفتيش وغيره.

وما تجدر الإشارة إليه في هذا الإطار أنه ليس أي معطيات معلوماتية محل إعتبار من المشرع، بل حصر المشرع الجزائري المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة في المعطيات المتعلقة بحركة السير (معطيات المرور)، وهي كما عرفها في المادة الثانية من القانون04/09 تلك المعطيات المتعلقة بالإتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة

---

(1)تجدر الإشارة إلى أنه من الأهمية بمكان التفرقة بين مصطلحي التحفظ على المعطيات la conservation des donneés والإحتفاظ أو أرشفة المعطيات l' archivge des données فرغم أن للكلمتين معنيين متجاورين في اللغة الشائعة لكن لهما معنى مختلف في اللغة المعلوماتية إذ أن عبارة يتحفظ على المعطيات تعني حفظ معطيات سبق وجودها في شكل مخزن وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها أو تجريدها من صفقتها أو حالتها الراهنة، في حين أن عبارة الإحتفاظ بالمعطيات تعني حفظ المعطيات لدى حائزها بالنسبة لمستقبل المعطيات التي في طور الإنتاج والتوالد ومعنى ذلك أن أرشفة المعطيات عبارة عن عملية تخزين للمعطيات على عكس التحفظ عليها الذي يعني النشاط الذي يضمن للمعطيات سلامتها وسريتها.

(2)آثر المشرع الجزائري إستعمال عبارة حفظ المعطيات في المادة 11 بدل التحفظ على المعطيات وذلك عكس ما فعلت إتفاقية بودابست في المادة 16 منها وهو بذلك إما أنه لايفرق بين المصطلحين أو أنه لا يقيم أهمية لمسألة ضمان أمن المعطيات من خطر التغير أو التجريد من صفقها أو حالتها الراهنة.

بإعتبارها جزءا في حلقة الإتصالات، توضح مصدر الإتصال،الوجهه المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الإتصال، ونوع الخدمة .وقد حصر المشرع معطيات المرور التي ألزم في المادة 11مزودي الخدمة بحفظها في:

1- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

2- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال.

3- الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال.

4- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

5- المعطيات التي تسمح بالتعرف على المرسل إليه الإتصال وكذا عناوين المواقع المطلع عليها.

وقد عرفت إتفاقية بوداسبت في مادها الأولى الفقرة "د"هذا النوع من المعطيات بأها صنف من بيانات الحاسوب التي تشكل محلا لنظام قانوني محدد، حيث يتم توالد هذه المعطيات من الحواسيب عبر تسلسل حركة الإتصالات لتحديد سلك الإتصالات من مصدرها إلى الجهة المقصودة، وهي بذلك تشمل طائفة من المعطيات تتمثل في مصدر الإتصال، ووجهته المقصودة خط السير، وقت أو زمن الإتصال، حجم الإتصال، ومدته ونوع الخدمة المؤداة. وبما أن حفظ المعطيات إجراء وقتي و إحتراما للحق في الخصوصية فان المشرع الجزائري وضع إلتزاما على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها بعد سنة من تاريخ التسجيل،(1)وعلى غرار المشرع الجزائري نجد المشرع الفرنسي حرص بدوره في نطاق التخزين التلقائي للمعطيات المتعلقة بالإتصالات الإلكترونية وذلك بموجب المادة 32 قانون البريد والإتصالات الإلكترونية المضافة بموجب المادة 29 من القانون رقم 1062/2001 والمعدلة بالمادة 20 من القانون 239/2003 المؤرخ في 2003/03/18 المتعلق بالأمن الداخلي على ضرورة مسح المعطيات المخزنة بعد الإحتفاظ بها لمدة أقصاها سنة إذا دعت مقتضيات البحث والتحقيق والمتابعة القضائية ذلك.

(1)المادة 11 من القانون 04/09 "...تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة إبتداء من تاريخ التسجيل.....".

وقد رتب المشرع الجزائري مسؤولية إدارية وأخرى جزائية على تقاعس مزودي الخدمة عن حفظ المعطيات المذكورة،[1] لإمكانية أن يشكل هذا التقصير عرقلة للسير العادي للتحريات القضائية.

وإسترشادا بما ذكر فإن مزودي لخدمة الأنترنات يعتبرون مصدرا لجهات البحث والتحقيق للحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها وملزمين في نفس الوقت بوضعها تحت تصرف هذه الجهات إذا ما تم طلبها.

(1) المادة 11 الفقرة الأخيرة"..... يعاقب الشخص الطبعي بالحبس من 06 أشهر إلى 05 سنوات وبغرامة من 50.000 دج ويعاقب الشخص المعنوي وفقا للقواعد المقررة في قانون العقوبات".

المبحث الثاني:

القواعد الإجرائيةفي إستخلاص الدليل الرقمي

لاشك أن التطور الحاصل في مجال المعلوماتية قد رتب آثارا هامة إنعكست على الجرائم من حيث الوسائل التي ترتكب بها، والمحل الذي تقع عليه، ونوع الجناة الذين يرتكبونها. وهذه الجرائم أي الجرائم المعلوماتية تجمع بين ذكاء المجرم (الذكاء الإنساني) وذكاء الأجهزة الرقمية (الذكاء الإصطناعي)، لذلك فإن هذا التطور التكنولوجي يجب أن يواكبه تطوير لقوانين العقوبات و قوانين الإجراءات الجزائية من أجل إستعاب الجرائم المستحدثة التي ترتكب عبر الوسائط الإلكترونية، كما يجب العمل على تطوير وسائل الإثبات الجزائية بما يتوافق والحقائق العلمية، فالقانون يجب أن لا ينفصل عن الواقع الذي أنتجه.(1)

والحاصل أنه مع ظهور الجرائم المعلوماتية التي تمثل ضربا من ظروب الذكاء الإجرامي، والتي باتت تتخذ أنماطا جديدة أصبح لا يجدي معها إتباع الطرق التقليدية في تحصيل الدليل لإثباتها لما تثيره طبيعتها غير المادية من إشكالات، وما تؤديه التقنية الحديثة من دور في إرتكابها، فإثبات الجرائم المادية التي تترك آثارا ملحوظة أمر سهل وميسور،بعكس إثبات الجرائم المعلوماتية ذات الطبيعة المعنويةبالنظر إلى أنها لا تترك آثار تدل عليها، على أساس أن أغلب البيانات والمعطيات التي تتداول عبر الحاسبات الآلية التي من خلالها تتم العمليات الإلكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحواسب التي تحفظها.

فالتطور التقني الذي لحق نظم المعالجة الآلية فضلا عن الطبيعة الخاصة للدليل الرقمي سيؤدي حتما ودون أي شك إلى تغيير كثيرٍ من المفاهيم السائدة حول إجراءات وطرق الحصول عليها، وهو الأمر الذي يحتاج بالضرورة إلى إعادة تقييم لمنهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية، فضلا عن إستحداث قواعد إجرائية أخرى تتلاءم مع طبيعة البيئة التقنية. فتطوير الإثبات ووسائله أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الإجرام،وهو الأمر الذي سوف نعالجة من حيث بحث القواعد الإجرائية التقليدية إلى أي مدى يمكن الإستناد إليها في

(1)عادل عزام سقف الحيط، المرجع السابق ص: 221،

الحصول على الدليل الرقمي، ثم نعرج إلى تدعيم المشرع جهات التحقيق بوسائل إجرائية مستحدثة تتفق وعملية البحث عن الدليل الرقمي من حيث طبيعته وطبيعة البيئة التي يتواجد بها.

المطلب الأول: القواعد الإجرائية التقليدية لاستخلاص الدليل الرقمي:

يصعب حتى هذه اللحظة في غالبية الأنظمة القانونية أن نحدد إلى أي مدى تكفي الأساليب التقليدية لإجراءات جمع الأدلة من أجل مباشرة تحقيقات ناجحة في مجال الجرائم المعلوماتية.(1)

ومما لا شك فيه أن المشرع لم يجز إستخلاص الدليل من غير ضوابط تحكم ذلك عن طريق قواعد إجرائية معينة أهمها: المعاينة، الخبرة، التفتيش وضبط الأشياء ومما لاشك فيه أيضا أن هذه القواعد عامة النطاق تنظم إستخلاص الدليل في جميع الجرائم، تقليدية كانت أم مستحدثة إلا أنها في الثانية قد تكون بحاجة إلى تطوير لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثباتها وهو ما سوف نعرفه من خلال ما يلي:

الفرع الأول: التفتيش وضبط الدليل الرقمي:

يجمع الفقه الجنائي على أن التفتيش هو إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في محل يتمتع بحرمة، وذلك وفقا للضمانات والقيود القانونية المقررة.

وأن ضبط الأدلة هو النتيجة الطبيعية التي ينتهي إليها التفتيش والتي يتم الحصول عليها أثناءه.

وعلى ذلك فإنه يتضح لنا أن هذين الإجرائين ما هما إلا وسيلة للإثبات المادي، ذلك أن التفتيش يستهدف ضبط أشياء مادية تساعد في إثبات وقوع الجريمة وإسنادها إلى المتهم المنسوب إليه إرتكابها. كما أن رجال الضبطية القضائية قد تعودوا في الجرائم التقليدية على ضبط إلا الأشياء المادية.

من أجل هذا فإن تفتيش نظم المعالجة الآلية يعد من أخطر المراحل حال إتخاذ الإجراءات الجزائية ضد مرتكب الجريمة المعلوماتية، لكون محل التفتيش فيها هو نظام المعالجة الآلية ذو الطابع غير المادي، ولا يعدو أن يكون إلا معلومات إلكترونية ليس لها أي مظهر مادي محسوس في العالم

---

(1) الرائد عبد الله حسين علي محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات بحث منشور على موقع: www.arablawinfo.com بدون ترقيم.

الخارجي.فما مدى صلاحية مكونات نظام المعالجة الآلية لأن تكون محلا يرد عليه التفتيش وما هي الأشياء المضبوطة في ظل التفتيش في العالم الإفتراضي؟

أولا: التفتيـــش في الـــبيئة الـــــرقمية:يثور التساؤل حول إمكانية تطبيق القواعد العامة للتفتيش على صورة تفتيش نظم الحاسوب والإنترنات، ذلك أن هذا الإجراء يهدف إلى جمع الأدلة المادية في حين أن نظم المعلوماتية عبارة عن كيان معنوي[1]ولا تتوافر له صفة المادة سواء تعلق ذلك ببرامجحاسوب أم ما يشمل عليه من بيانات.

لكن من المعروف أن نظم المعالجة الآلية تتكون من مكونات مادية وأخرى غير مادية ترتبط بغيرها عبر شبكات إتصال بعدية على المستوى المحلي أو الدولي[2]

وإذا كان التفتيش هو التنقيب في وعاء السر بقصد ضبط ما يفيد من الأسرار في كشف الحقيقة، وأن جوهره هو كشف نقاب السرية عما تحويه نظم المعالجة الآلية من خفايا وأسرار ونوايا إجرامية، وبالتالي إزاحة ستار الكتمان عنها للإستفادة منها في معرفة الحقيقة. واذا كان هذا المعنى لا يتقيد بالكيان المادي لوعاء السر، فإن الأمر يتطلب منا البحث في مسألة المحل الذي ينصب عليه هذا الإجراء التحقيقي في مجال المعلوماتية.

1/محل التفتيش في البيئة الرقمية:يتكون النظام المعلوماتي من مكونات مادية (HARD WARE)ومكونات منطقية (SOFT WARE)،كما أن له شبكات إتصالات بعدية سلكية ولا سلكية على المستوى المحلي والدولي فهل تخضع هذه المكونات للتفتيش؟

1.1/تفتيش المكونات المادية لنظام المعالجة الآلية:إن التفتيش الواقع على المكونات المادية للنظام المعالجة الآلية لا توجد فيه أي مشكلة في التنفيذ لإمكانية ذلك وسهولته، مع الأخذ بعين الإعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها، وتأتي سهولة هذا التفتيش لأنه يرد على أشياء مادية لا خلاف حول خضوعها للتفتيش طبقا لقواعد قانون الإجراءات الجزائية الخاصة بهذا الاجراء. ففي نص المادة 44 من قانون الإجراءات الجزائية ورد بالمعنى أن التفتيش يرد على الأشياء، وهي كلمة تنصرف في الأرجح على المكونات المادية ونفس

([1])علي حسن محمد الطوالبة،التفتيش الجنائي على نظم الحاسوب و الإنترنات،عالم الكتب الحديثة .الأردن 2004 ص7.

([2])رشيدة بوكر، المرجع السابق.ص394،

القول ينصرف على ما جاءت به المادة 64 من نفس القانون بنصها: لا يجوز تفتيش المساكن... وضبط الأشياء..."

وعلى هدي ذلك فإنه لا يوجد مانع قانوني من أن ينصب التفتيش على المكونات المادية للحاسوب وملحقاتهاأومعداته، وذلك تبعا لطبيعة المكان الذي يتواجد فيه الحاسوب وهذه الملحقات، سواء من الأماكن العامة أو من الأماكن الخاصة، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت خاصة كمسكن المتهم أو أحد ملحقاته كانت لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانونا.[1]

إلا أن المشرع الجزائري بمناسبة التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون 22/06المؤرخ في20 ديسمبر 2006إستثنى بموجب الفقرة الثالثة من المادة 45 وكذا الفقرة الثانية من المادة 47 والفقرة الثالثة من المادة 64 تطبيق هذه الضمانات عند إجراء التفتيش بمناسبة تحقيق مفتوح بخصوص الجرائم المعلوماتية.

ويفهم من إستقراء هذه المواد أن المشرع لا يشترط حضور الشخص الذي يشتبه في أنه ساهم في إرتكاب الجريمة عند تفتيش مسكنه،[2]وأنه يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل[3]و ودون حاجة إلى رضائه عند القيام بهذا الإجراء.[4]

والملاحظ أن الشرع في هذه الحالة قد غلب المصلحة العامة على حريات الأفراد، و مرد ذلك إلى إعتبارين:

-ذاتية الجريمة المعلوماتية المتمثلة في إمكانية إختفائها بسرعة فائقة.

-إفتراض كون الدليل الرقمي هو الدليل الوحيد في الدعوى الجزائية ومن ثم إرتكاز كل العملية الإثباتية على وجوده.

([1])نصت المادة 64 من ق إج أنه لا يجوز تفتيش المساكن....إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات..." فضلا عن ما ورد في المواد من 44 إلى 47 من نفس القانون.

([2])الفقرة 03 من المادة 45 تنص على أنه "لا تطبق أحكام هذه المادة إذا تعلق الأمر بالجرائم ....أنظمة المعالجة الآلية للمعطيات".

([3])الفقرة 03 من المادة 47 تنص على:" عندما يتعلق الأمر بـــ.....الجرائم المادة بأنظمة المعالجة الآلية للمعطيات .....فإنه يجوز إجراء التفتيش..... في كل محل مسكن أو غير سكني في كل ساعة من ساعات النهار أو الليل....".

([4])الفقرة الثانية من المادة 64"..... وتطبق فضلا عن ذلك أحكام المواد 44 إلى 47 من هذا القانون" أي عدم تطبق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بجرائم المعلوماتية.

2.1/تفتيش المكونات المعنوية لنظام المعالجة الآلية:إذا كان الأمر قد إنتهى بنا إلى صلاحية المكونات المادية للنظم المعلوماتية كمحل يرد عليه التفتيش، فإن إمتداد ذلك إلى مكوناته غير المادية هو محل جدل كبير حول مدى صلاحيتها لأن تكون موضوعا للتفتيش تمهيدا لضبط الأدلة.

فالخلاف حاصل في مسألة أن التفتيش التحقيقي وسيلة للبحث عن الأدلة المادية، إذ هو إجراء يسعى إلى ضبط الأدلة المتعلقة بالجريمة لتقديمها إلى المحكمة المختصة كدليل إدانة، لذلك يثور الشك والتساؤل حول إمكانية إعتبار البحث عن أدلة الجريمة المعلوماتية في نطاق نظم الحاسوب نوعا من التفتيش بإعتبار أن البيانات الإلكترونية أو البرامج في حد ذاتها ليس لها مظهر مادي محسوس في المحيط الخارجي ويستشعر الفقه صعوبة المسألة نظرا لغياب الطبيعة المادية للمعلومات في ذاتها مجردة من دعامتها المادية.[1]وقد ذهب الفقه بهذا الشأن مسارين رئسين:

المسار الأول: تتمثل فكرته في عدم إمكانية إنسجام وتطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية من بحث وتنقيب عن الأدلة في برامج الحاسوب وبياناته.

فهناك جانب من التشريعات الإجرائية قد حدد هدف التفتيش في البحث عن الأشياء وضبطها، وهذا الشيء يقتصر بمفهومه على المال ذي الحيز المادي المحسوس ولا يمتد في نطاق شموله إلى الكيانات المنطقية، وقد عملت الدول التي أخذت بهذا الإتجاه إلى حماية هذه الكيانات المنطقية عبر قوانين الملكية الفكرية.[2]

المسار الثاني: يخلص أصحاب المسار إلى أن برامج الحاسوب يمكن أن تنطبق عليها خصائص وسمات المادة، وبالتالي تدخل في نطاق الأشياء المادية ويستوي في ذلك أن تكون برامج نظام أو برامج تطبيقات،[3]مستندين في ذلك إلى أن المادة هي كل ما يشغل حيزا ماديا في فراغ معين، وأن هذا الحيز يمكن قياسه والتحكم فيه وبناءا عليه فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ويمكن قياسه بمقياس معين هو البايت (Byte) والكيلوبايت (kb) والميغابايت(MB)، وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسوب بعدد الحروف التي

---

(1)عبد العظيم وزير، شرح قانون العقوبات القسم الخاص جرائم الإعتداء على الأموال الطبعة الأولى، دار النهضة العربية القاهرة 1993، ص40.

(2)علي حسن محمد الطوالبة، المرجع السابق ص31..

(3)هلالي عبد اللاه أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي.دراسة مقارنة. دار النهضة العربية.القاهرة 2006 ص75 وما بعدها .

يمكن خزنها فيها.[1]لذلك ذهب الفقه في تفسيره إلى الإستناد على الربط بين النصوص الإجرائية التي أوردت عبارة "أي شيء"[2]والتي يقصد بها المادة وبين العلوم الطبيعية ومفهومها في البيانات المنطقية أو البرامج.

غير أن النصوص القانونية التي أرست القواعد التي تحكم التفتيش تم سنها قبل أن يعرف القانون الأشياء غير المادية، لكن تقدم الفكر البشري والتطور الذي رافقه أظهر للوجود قيما إقتصادية وأشياء غير مادية ليس لها حيز محسوس، لذلك فأيا كانت المبررات التي ساقها معتنقوا المساواة بين الكيان المادي ونقيضه فإن طبيعة البيانات والمعطيات المعالجة تتطلب قواعد خاصة تحكمها بدلا من محاولة تطويع القواعد التقليدية وتوسيع نطاقها، وهذا يتأتى من خلال إجراء تعديل عليها من شأنه توسيع نطاق الأشياء التي تكون مشمولة بالتفتيش وتضمينها من الأحكام بما يتلاءم ومتطلبات هذه التقنية الجديدة ،فالنصوص الخاصة بالتفتيش بمعناه التقليدي لا يمكن إعمالها مباشرة على النظم المعلوماتية لأن قياسها على الأشياء المادية سيكون منافيا للشرعية الإجرائية.

ويتضح موقف المشرع الجزائري من خلال القانون 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، حينما أجاز صراحة تفتيش المنظومات المعلوماتية، وذلك بموجب المادة 05 منه التي نصت على أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية.... الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين معلوماتية.

وإلى جانب المشرع الجزائري قام المشرع الفرنسي بتعديل النصوص التي تحكم التفتيش وأضاف عبارة "المعطيات المعلوماتية" في المادة 94 من قانون الإجراءات الجزائية بموجب المادة 42 من القانون رقم 2004/545 المؤرخ في 2004/06/21 المتعلق بالثقة في الإقتصاد الرقمي ليصبح نص

([1])وما يؤيد هذا الرأي أن هذه البيانات تكون على شكل نبضات إلكترونية وهي في هذا تشبه التيار الكهربائي الذي إعتبرته بعض التشريعات أشياء مادية منقولة وعاقبت على الإستخدام القانوني له.

([2])فالمادة 487 من القانون الكندي تقضي بإمكانية إصدار أمر قضائي لتفتيش وضبط أي شيء تتوافر بشأنه أسس ومبررات معقولة تدعو إلى الإعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها أو هناك نية لإستخدامه في إرتكاب الجريمة أو أنه يستنتج دليلا على وقوع الجريمة فإن الفقه الكندي في تفسيره لهذه المادة وسع من نطاقها إلى حد يسمح بتفتيش بيانات ونظم الحاسوب غير المادية .

هذه المادة على النحو التالي:" يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة".

وينص القانون الإنكليزي المتعلق بإساءة إستخدام الحاسوب على جواز تفتيش نظم الحاسوب المادية والمعنوية، وإعتبر هذا القانون أن إجراءات تفتيش نظم الحاسوب في جرائم الولوج أو التعديل غير المصرح به على أنظمة الحاسوب تتم دون إذن طالما كان هدف الولوج إرتكاب أفعال غير مشروعة عن قصد، أما إذا كان الولوج مجردا دون نية إرتكاب أفعال غير مشروعة فإن التفتيش ممكن ولكن بإذن قضائي.

وفي هذا الصدد صرحت الإتفاقية الأروبية في شأن جرائم تقنية المعلومات بحق الدول الأعضاء في تفتيش النظم في إطار الإجراءات الجزائية، وذلك من خلال الفقرة الأولى من المادة 19 من القسم الرابع أين نصت على أنه لكل دولة طرف الحق في أن تسن من القوانين ما هو ضروري لتمكين السلطات المختصة بالتفتيش أو الدخول إلى:

- نظام الكومبيوتر أو جزء منه أو المعلومات المخزنة فيه.
- الوسائط التي يتم تخزين معلومات الكومبيوتر بها ما دامت مخزنة في إقليمها.

3.1/تفتيش الشبكات المعلوماتية المتصلة بالحاسوبّ التفتيش عن بعد": تعرف الشبكة المعلوماتية بأنها مجموعة مكونة من إثنين فأكثر من أجهزة الحاسوب والمتصلة ببعضها إتصالا سلكيا أو لا سلكيا.[1]وقد تكون الأجهزة موجودة في نفس الموقع وتسمى بالشبكة المحلية (local Area Net worh-LAN)،وقد تكون موزعة في أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف وتسمى بالشبكة بعيدة المدى (Wide Area-Net werh-WAN). [2]

([1])علي حسن محمد الطوالبة المرجع السابق.، ص34

([2])يتم الإتصال أو نقل المعلومات بواسطة الشبكية بأشكال ثلاث هي:

إتصال أحادي الجانب (Simplex) ويتم هذا الإتصال بين جهاز الحاسوب المستفيد مع جهاز مركزي.

إتصال ثنائي غير كامل المعلومات (Half Duplex) ويتم الإتصال بين جهازين يرسل الأول المعلومات والثاني يستقبلها وبعد إنتهاء الأول يقوم الثاني بإرسال المعلومات ويستقبلها الأول وهكذا لكن لا يستطيع الإثنان التخاطب "الإرسال والإستقبال" في آن واحد.

إتصال ثنائي كامل المعلومات (Full Duplex) ويتم الإتصال بواسطته بين جهازين الإرسال والإستقبال في نفس الوقت.

ومع التطور التكنولوجي لثورة الإتصالات لم يعد نطاق الإتصالات محدودا في إقليم دولة واحدة، بل إمتد ليشمل كل أرجاء العالم بعد ظهور شبكة الأنترنات والتي هي عبارة عن منظومة واسعة جدا من شبكات المعلومات الحاسوبية المتصلة مع بعض البعض بطريقة لا مركزية، ويدخل في تركيب هذه الشبكة ملايين الحواسيب الموزعة عبر مختلف دول العالم.

والسؤال المطروح في هذا الصدد يتعلق بمدى خضوع شبكات نظام المعالجة الآلية للتفتيش وهي مسألة على درجة كبيرة من الخطورة تتعلق بالتفتيش عن بعد(Perquisitionsadistence) وذلك نتيجة للطبيعة التكنولوجية الرقمية التي تسمح بتوزيع المعلومات التي تحتوي أدلة عبر شبكات حاسوبية في أماكن مجهولة بعيدا تماما عن الموقع المادي للتفتيش،فقد يكون الموقع الفعلي للشبكات داخل إختصاص قضائي آخر وحتى في بلد آخر، وهو ما يزيد المسألة تعقيدا بإعتبار أن الشبكة المعلوماتية ممتدة في أرجاء العالم تقريبا، وبالتالي فإن الحاسوب أو النهاية الطرفية التي يمكن أن ترتكب عليها أو بواسطتها الجريمة المعلوماتية تخضع للقانون الإجرائي الخاص بتلك المنطقة.(1)

لذلك يثار التساؤل حول أثر تفتيش الأنظمة المعلوماتية المتصلة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر إختصاص مختلفة. ونستطيع أن نميز في هذه الصورة بين إحتمالين على النحو التالي:

1.3/إتصال حاسب المشتبه فيه أو المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة،وهنا يثور التساؤل حول مدى إمكانية إمتداد الحق في التفتيش إلى أجهزة الحاسوب المتصلة بجهاز المشتبه فيه أو المتهم. وفي هذه الحالة عمدت بعض التشريعات الإجرائية إلى حل هذه المشكلة من خلال نصها على إجازة تفتيش نظم المعلومات المتصلة بالحاسوب الذي يجري تفتيشه (أي الشبكة وما يتصل بها)، وتسجيل كل البيانات اللازمة كأدلة إثبات لإدانة المتهم أمام المحكمة.

ويعتبر المشرع الجزائري من بين هذه التشريعات حين نصت الفقرة الثانية من المادة 05 من القانون 04/09 بأنه في حالة تفتيش منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها إنطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك".

---

(1)علي حسن الطوالبة، المرجع السابق ص42،.

وإلى جانب المشرع الجزائري نجد المشرع الألماني في المادة 103 من قانون الإجراءات الجزائية الألماني ينص على إمكانية إمتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر، وكذلك المشرع البلجيكي في المادة 88منقانون تحقيق الجنايات البلجيكي التي تنص على" إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي أو في جزء منه فإن البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي."(1)

والمشرع الفرنسي حسم هذه المسألة أيضا بمناسبة تعديله قانون الإجراءات الجزائية بموجب القانون 2003/239 المتعلق بالأمن الداخلي الصادر في 2003/03/18 الذي أجازت المادة 17 منه لضباط الشرطة القضائية أو تحت مسؤولياهم أعوان الشرطة القضائية في إطار التفتيش المنصوص عليه الدخول عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي فيها التفتيش على المعطيات التي تهم التحقيق والمخزنة في النظام المذكور أو في أي نظام معلوماتي آخر، بما أن هذه المعطيات يتم الدخول إليها أو تكون متاحة إنطلاقا من النظام الرئيسي(2)

وتسمح الإتفاقية الأوروبية لجرائم تقنية المعلومات لعام 2001 للدول الأعضاء أن تمد نطاق التفتيش الذي كان محله جهاز كومبيوتر معين إلى غيره من الأجهزة المرتبطة به في حال الإستعجال إذا كان يتواجد به معلومات يتم الدخول إليها في هذا الجهاز من خلال الجهاز محل التفتيش(3).

2.3/إتصال حاسب المشتبه فيه أو المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة، وهنا من المتصور طبقا لهذا الإحتمال أن يقوم مرتكبوا الجرائم بتخزين بياناتهم في أنظمة معلوماتية خارج الدولة عن طريق شبكات الإتصال البعيدة بهدف عرقلة سلطات التحقيق في جمع الأدلة.(4)

(1)خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص203.

(2)voire plus Myriam QUENER.joél FERRY. Cybercriminalité Défi mondial 2em edition 2009 p2

(3)تنص المادة 2/19 من القسم الرابع على أنه من حق السلطة القائمة بتفتيش الكومبيوتر المتواجد في دائرة إختصاصها أن تقوم في حالة الإستعجال بمد نطاق التفتيش إلى أي جهاز آخر إذا كانت المعلومات المخزنة يتم الدخول إليها من الحاسب الأصلي محل التفتيش.

(4)عبد الله حليس علي محمود، إجراءات جمع الأدلة في مجال سرقة المعلومات بحث منشور على موقع:www.arablawinfo.com

فمن المشاكل الحقيقية التي تواجه جهات التحقيق في جمع الأدلة، حالة تطلب إمتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر عن جهاتها المختصة الإذن بالتفتيش، ودخوله في المجال الجغرافي لدولة أخرى. وهو مايسمى بالتفتيش العابر للحدود، وقد يتعذر القيام به بسبب تمسك كل دولة بسيادتها وحدودها الإقليمية.

لذا فإن جانبا من الفقه يرى أن التفتيش الإلكتروني العابر للحدود ينبغي أن يتم في إطار إتفاقيات تعاون خاصة ثنائية أو دولية تجيز هذا الإمتداد، وأنه لا يجوز القيام به في ظل غياب تلك الإتفاقيات،(1)ووفقا لما جاء بتقرير المجلس الأروبي فإن الإختراق المباشر يعد إنتهاكا لسيادة دولة أخرى ما لم توجد إتفاقية دولية في هذا الشأن، فإسترجاع البيانات التي تم تخزينها بالخارج دون علم الدولة الأخرى أو رضاها يعد إنتهاكا السيادة للدولة الأخرى وخرقا للقوانين.

ولمواجهة هذا الإحتمال نجد أن المشرع الجزائري قد أجاز تفتيش الأنظمة المتصلة حتى ولو كانت متواجدة خارج الإقليم الوطني، وهو الوارد بالفقرة الثالثة من نص المادة 05 من القانون04/09"... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها إنطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للإتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل". ولعل هذه الفقرة مأخوذ نصها من الفقرة الثانية من المادة 57-1 من قانون الإجراءات الجزائية الفرنسي(2)

وفي نفس الإطار أصدر المجلس الأروبي توصية تحمل رقم 13 لسنة 1995 والمتعلقة بالمشكلات القانونية لقانون الإجراءات الجزائية المتصلة بتقنية المعلومات يجيز من خلالها أن يمتد تفتيش الحاسوب إلى الشبكة المتصلة بها ولو كانت تلك الشبكة تقع خارج إقليم الدولة.

ولكن طالما أن التفتيش عن بعد يمتد إلى إقليم بلد أجنبي فإن الأمر يستلزم بالضرورة الدخول في إطار بحث هذا الإختراق المباشر على مستوى الدول كافة بإعتباره إجراء عابرا للحدود وهو

---

(1)محمد أبو العلا عقيدة. التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية، بحث مقدم للمؤتمر العلمي الاول حول الجوانب القانونية و الامنية للعمليات الالكترونية.اكاديمية الشرطة.مركز البحوث و الدراسات.دبي خلال الفترة 28/26افريل2003. منشور على موقع www.arablaw info.com، ص10.

(2)المادة 57-2/1 من قانون الإجراءات الجزائية الفرنسي مضافة بموجب المادة 2/17 من القانون 2003/239"إذا تبين مسبقا أن هذه المعطيات مخزنة في نظام معلوماتي موجود خارج الإقليم الوطني وأنه يمكن الدخول إليها وأنها متاحة إنطلاقا من النظام الرئيسي فإنه يمكن الحصول عليها من طرف ضباط الشرطة القضائية مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية".

الأمر الذي لا يخلو من ضرورة التوصل إلى إتفاق دولي يضمن التعاون الدولي فيما بين السلطات المختصة، والقول بغير ذلك يجعل من هذا الإجراء تهديدا لسيادة الدول.

إلا أنه وبالرغم من ذلك فإن الإتفاقية الأوروبية الخاصة بجرائم تقنية المعلومات أجازت في المادة 32 منها إمكانية الدخول بغرض التفتيش إلى أجهزة وشبكات تابعة لدولة أخرى بدون إذنها في حالتين:"

- إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور.
- إذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش.

2/شروط التفتيش في البيئة الرقمية:

لقد حرصت القوانين الإجرائية على إحاطة إجراء التفتيش بشروط وضمانات أساسية نظرا لما يمكن أن يحدثه من مساس يحق الإنسان في حريته الشخصية، وهدف ذلك هو تحقيق الموازنة بين مصلحة المجتمع في عقاب المجرم وبين حقوق الأفراد وحرياتهم.ومن الشروط والضمانات التي يجب توافرها منها ما هو موضوعي ومنها ما هو شكلي.

1.2/الشروط الشكلية للتفتيش في البيئة الرقمية:

إن القواعد الشكلية لا تهدف إلى تحقيق مصلحة العدالة في ضمان صحة الإجراءات التي تتخذ لجمع الأدلة فحسب، وإنما تقيم بالإضافة إلى مقتضيات الإجراء سياجا يحمي الحريات الفردية.(1)ولعل أبرز هذه الشروط هي:

1.1/ إجراء التفتيش بحضور أشخاص معينين بالقانون:غني عن البيان أن التفتيش فيه إطلاع على أسرار الغير التي تحرم أغلب التشريعات الإجرائية الإطلاع عليها، لذلك فإنه ومن مطالعة التشريعات المقارنة نجد أن بعضها أوجب حضور عملية التفتيش الذي تجريه الضبطية القضائية المشتبه فيه أو شهودا.وأوجبتتشريعات أخرى حضور أشخاص معينين في القانون في حالات معينة، وأجازت في أحوال أخرى إجراء التفتيش دون حضور أحد، وهناك تشريعات سكتت تماما عن التعرض لهذا الشرط.

(1) علي حسن الطوالبة، المرجع السابق ص47،

وإن كان المشرع الجزائري من التشريعات الإجرائية التي أوجبت ضرورة حصول إجراء التفتيش المتعلق بالمساكن وملحقاتها بحضور المشتبه فيه عندما يتم تفتيش مسكنه من طرف الضبطية القضائية، وإن تعذر ذلك بإمتناعه عن حضور التفتيش أو كان هاربا يتم هذا الإجراء بحضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائية القائم بالتفتيش،(1)إلا أنه وبموجب التعديل الذي ألحقه على قانون الإجراءات الجزائية بالقانون 22/06.إستثنى تطبيق هذه الشروط (حضور المشتبه فيه أو الشاهدين عندما يتعلق الأمر بالجرائم المعلوماتية)،(2)وهو ما يعد إقرارا من المشرع بذاتية هذا النوع من الجرائم وما يتطلبه التحقيق بشأنها من بسط نوع من السرية أثناء جمع الدليل الرقمي بالإضافة إلى الإسراع في إستخلاصه قبل فقدانه.

ونجد تطبيق ذلك في الولايات المتحدة الأمريكية حيث تصدر السلطة المختصة بالتحقيق أوامر التفتيش دون إخطار مسبق في الدعاوى المتعلقة بالجرائم المعلوماتية، وذلك خوفا من سهولة تدمير المعلومات الموجودة على ذاكرة الحاسوب بما قد يضر بحسن سير إجراءات التحقيق

2.1/الميعاد الزمني لإجراء التفتيش في البيئة الرقمية:

إختلفت التشريعات الإجرائية في وقت تنفيذ التفتيش، فمنها ما يحظر تفتيش المساكن ليلا إلا في أحوال معينة، ومنها لم يقيد القيام بهذا الإجراء بوقت معين وترك الأمر لتقدير القائم بالتفتيش لإختيار الوقت الملائم لتنفيذه ضمن المدة المحددة بالإذن.(3)

والمشرع الجزائري ذهب إلى حضر تفتيش المساكن وما في حكمها في أوقات معينة وحدد ميقات تنفيذ هذا الإجراء من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا،(4)وهناك حالات إستثنائية يجوز فيها الخروج عن هذا الميقات ويصح إجراؤه في أي ساعة من ساعات الليل والنهار عندما يتعلق الأمر بالتحقيق في الجرائم المنصوص عليها بالمواد342 إلى348 من قانون العقوبات المرتكبة في أماكن معينة(5)أو في حالة رضا صاحب المسكن صراحة.

---

(1)أنظر نص المادة 45 من قانون الإجراءات الجزائية.

(2)أنظر الفقرة الأخيرة من المادة 45 ق.إ.ج.

(3)أنظر قانون الشرطة والأدلة الجنائية البريطاني لسنة 1984.

(4)المشرع الفرنسي من خلال المادة 59 ق.إ.ج يحدد ميقات تنفيذ التفتيش من الساعة السادسة إلى الساعة التاسعة مساءا.

(5)المادة 47 ق.إ.ج.

وفي نطاق التفتيش المتعلق بالجرائم المعلوماتية فإن الإستثناء الوارد بالفقرة الثالثة من المادة 47 ق.إ.ج والمتعلق بجواز إجراء ضابط الشرطة القضائية للتفتيش في كل ساعة من ساعات الليل أو النهار عندما يتعلق التحقيق بنوع معين من الجرائم، فقد شمل هذا الإستثناء الجرائم المعلوماتية حيث جاء في نصها"**....** عندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و **...** فإنه يجوز إجراء التفتيش**...**في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص".

2.2/الشروط الموضوعية للتفتيش في البيئة الرقمية: يمكن تحديد القواعد الموضوعية لتفتيش نظم الحاسوب والتي تعد الضوابط اللازمة لإجراء تفتيش صحيح في ما يلي:

1.2/وجود سبب للتفتيش: إن سبب التفتيش في القواعد العامة بوصفة إجراء من إجراءات التحقيق هو وقوع جريمة (جناية أو جنحة) وإتهام شخص أو عدة أشخاص بإرتكابها أو المساهمة فيها، وتوافر أمارات وقرائن قوية على وجود أشياء في كشف الحقيقة لدى المشتبه فيه أو غيره(1)وبناءا عليه وتطبيقا على الجرائم المعلوماتية فإن سبب التفتيش المتعلق بهذا النوع من الجرائم يعني:

- ضرورة وقوع جريمة من الجرائم المعلوماتية التي نص عليها المشرع في نصوص التجريم والعقاب طبقا لمبدأ شرعية الجرائم والعقوبات، كما هو الحاصل في التشريع الجزائري الذي أدرج فصلا خاصا -الفصل السابع- في قانون العقوبات لجرائم الإعتداء على نظم المعالجة الآلية للمعطيات، ذلك أن التفتيش الذي يقع من أجل فعل لا يشكل جريمة يعتبر باطلا، بالإضافة إلى أن تكون هذه الجريمة قد وقعت فعلا فلا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة مستقبلية ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل، إلا أنه وبالرجوع الى نص المادة 05 من القانون 04/09 نجد ان المشرع قد اجاز إمكانية اللجوء الى إجراء تفتيش النظام المعلوماتي إما

---

(1)وهو ما أقرته محكمة النقض المصرية بإعتبارها أن الإذن بالتفتيش لا يصح إصداره إلا لضبط جريمة واقعة بالفعل وترجحت نسبتها إلى متهم معين وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية .طعن نقض جنائي جلسة 1967/10/16 مجموعة أحكام النقض س18 رقم 195، ص965.

للوقاية من حدوث جرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينة ذكرها المادة االرابعة من نفس القانون، وهو الامر الذي يفهم صراحة بقراءة نص المادتين معا.

- ضرورة الإشتباه في شخص معين أو إتهامه بإرتكاب الجريمة أو المشاركة فيها،فلا يكف لقيام سبب التفتيش وقوع جريمة معلوماتية بل لابد أن يكون هناك إتهام موجه ضد شخص معين أو أن تتوافر دلائل كافية تدعو للإعتقاد بإرتكابه للجريمة حتى يمكن إنتهاك حق الخصوصية لديه وتفتيش حاسوبه الشخصي وبرامجه الخاصة ويمكن الإستدلال على ذلك بما نصت عليه المادة 46 ق.إ.ج" لا يجوز لضباط الشرطة القضائية الإنتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية ويحوزون أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء التفتيش...." ومن الدلائل المستمدة من الواقع والقرائن التي تنبئ عن إرتكاب الشخص لجريمة معلوماتية وترجح إمكانية نسبتها له وفق السياق العقلي والمنطقي أن يتم تحديد هوية الحاسوب (IP) الذي تم إرتكاب الجريمة به وكان ذلك الحاسوب يخص شخصا بعينه.

2.2/تحديد محل التفتيش: يقصد بمحل التفتيش المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سره، ومحل التفتيش في الجرائم المعلوماتية هو نظام المعالجة الآلية بكل مكوناته المادية والمعنوية وشبكات الإتصال كما سبق شرحه وبيانه.

وحكم تفتيش هذه المكونات يتوقف على طبيعة المكان الموجود فيه، فيما إذا كان من الأماكن العامة أم من الأماكن الخاصة، وتكمن أهمية التفرقة هنا في أن هذه الكيانات في الأماكن الخاصة يكون لها حكم تفتيش المساكن بنفس الضمانات المقررة قانونا سيما إشتراط الإذن بالتفتيش من السلطات القضائية المختصة وهو ما نصت عليه المادة 44 من قانون الإجراءات الجزائية أنه لا يجوز لضباط الشرطة القضائية الدخول إلى المساكن وإجراء التفتيش إلا بإذن مكتوب من وكيل الجمهورية أو من قاضي التحقيق، وهذه الضمانة خاصة بجميع الجرائم بما فيها الجرائم المعلوماتية. أما التفتيش الواقع على مكونات الحاسوب الموجودة في الأماكن العامة فإن أغلب الشريعات تجيز لرجال الضبطية دخول المحال العامة المفتوحة للجمهور كمقاهي الأنترنات من أجل مراقبتها والتأكد من إحترامها للأخلاق والآداب العامة بكل سهولة دون حاجة لإذن بالتفتيش(1)

---

(1) علي حسن محمد الطوالبة، المرجع السابق ص81.

3.2/الإذن بالتفتيش: يثور التساؤل حول إمكانية تطبيق القواعد العامة في التفتيش على صورة تفتيش نظم الحاسوب، علما أن التفتيش التقليدي يهدف إلى جمع الأدلة المادية في حين أن نظم الحاسوب عبارة عن كيان معنوي ولا تتوافر له صفة المادة، ولما كان محل التفتيش بصورته التقليدية المساكن والأماكن الملحقة بها، فقد أضفى عليها القانون الإجرائي حماية خاصة بإعتبارها مكنونا لسر الأفراد ومحلا لخصوصياتهم، ومن الضمانات المقررة في الشريعات الإجرائية الجزائية أنه لا يجوز تفتيش المساكن أو الشروع في تفتيشها إلا بإذن مكتوب من السلطة القضائية المختصة .

والسؤال المطروح هنا هل يمكن إعمال ذات الشرط عندما يتعلق الأمر بتفتيش منظومة معلوماتية أو جزء منها؟ أي هل يمكن القول أنه لا يجوز الولوج إلى البيئة الرقمية والقيام بتفتيشها من طرف الضبطية إلا بإذن مكتوب من السلطة القضائية المختصة؟ أو بمعنى آخر ما مدى اشتراط إذن بالتفتيش خاص بالنظام المعلوماتي.

غالبا ما يصدر الإذن بتفتيش مسكن المتهم وينصرف هذا الإذن إلى كل ما يتواجد في المسكن ومن ثم فهل يجوز بمتقضى هذاالإذن لضباط الشرطة القضائية الولوج إلى البيئة الرقمية والتغلغل في المنظومة المعلوماتية للبحث عن الأدلة الإثباتية التي يمكن أن تكون محل ضبط؟

إنه من المستقر عليه في التشريعات المقارنة كالقانون الامريكي مثلا لا يجيز تفتيش جهاز الكومبيوتر الا بناء على إذن وفقا للصل العام .أما المشرع الجزائري فإنه في اعتقادنا لم يقدم حلا لهذه المسألة بصورة صريحة، ذلك أن القواعد الخاصة بإجراء التفتيش المذكورة في قانون الإجراءات الجزائية تتعلق بالتفتيش التقليدي الذي محله المساكن وملحقاتها، وأن القواعد الخاصة بإجراء التفتيش المعلوماتي الواردة بالقانون 04/09 لا نجد الشرع يتحدث عن هذا الشرط إطلاقا، كل ما في الأمر أنه تحدث عن إعلام جهات التحقيق السلطة القضائية المختصة في حالة تمديد التفتيش إلى منظومة معلوماتية أخرى.

فهل يعني هذا السكوت من طرف المشرع أنه يجوز تفتيش المنظومة المعلوماتية دون حاجة إلى إذن آخر بالتفتيش يخص المنظومة المعلوماتية ويكفي فقط الإذن المتعلق بالمسكن الذي يتواجد فيه الحاسوب؟

وطبقا لمعيار الخصوصية التي يحميها المشرع فإن النظام المعلوماتي وما يحتويه من أسرار وخصوصيات الأشخاص، فإنه يخضع بالتبعية لمبدأ عدم جواز الدخول إلى هذا النظام المعلوماتي

وتفتيشه دون إذن من السلطة القضائية المختصة، ومؤدى ذلك أن ضابط الشرطة القضائية من أجل تفتيش منظومة معلوماتية فإنه يحتاج في الغالب إلى إذنين بالتنفتيش، الأول يخص المسكن الذي يتواجد به الحاسوب والثاني يتعلق بتفتيش المنظومة المعلوماتية في حد ذاتها أو على الأقل إذنا واحدا يجيز لضابط الشرطة القضائية تفتيش جهاز الكومبيوتر الخاص بالتهم إلى جانب تفتيش السكن.

4.2/تحديد مجال الإذن بالتفتيشيتجه الرأي الغالب في التشريعات المقارنة على غرار المشرع الجزائري إلى تطلب شرط التحديد لصحة الإذن بالتفتيش إذ نصت المادة 44 "**.....**يجب أن يتعين الإذن بالتفتيش بيان وصف الجرم وعنوان الأماكن التي يتم زيارتها وتفتيشها وذلك تحت طائلة البطلان"**.**وفي نطاق تفتيش الأنظمة المعلوماتيةفمن المعلوم أن التخزين هو البيئة التي تتصف بها الحوسبة أو الرقمية، فالبيئة الرقمية بهذه الصفة تعد مجالا ضخما يمكنه تخزين مليارات المعلومات والملفات، من أجل هذا فإن صياغة الإذن بالتفتيش الخاص بالبيئة الرقمية وحتى تنفيذه يشكلان تحديات كبيرة إذ أن المادة المطلوبة قد تختلط بكميات هائلة من البيانات الأخرى التي لا تناسب الموضوع قيد التحقيق، لذلك فإنه لا يستقيم الأمر مع مبدأ الخصوصية أن يطلع ضابط الشرطة القضائية على جميع البيانات الشخصية الموجودة بالحاسوب، كما أن ضبط النظام برمته قد يسبب خسارة غير واجبة للمشتبه فيه(1)

وبالتالي لا يفيد التفتيش أن يكون شاملا وإنما ينبغي أن يكون أكثر تخصصا لكي يكون مبررا**.**ولا شك أن في تحديد إذن التفتيش تحديدا دقيقابالنسبة للجرائم المعلوماتية قد يخلق صعوبة أثناء الممارسة العملية في تفتيش نظم المعالجة الآلية، ويرجع ذلك كما ذكرنا إلى الطبيعة الخاصة لهذه الأخيرة من حيث كونها تحتوي على عدد كبير من الملفات وهو ما يثير التساؤل حول ما إذا كان كل ملف يلزم معاملته كصندوق مغلق يحتاج كل واحد منها إلى إذن قضائي مستقل عن الآخر(2)

والمشرع الجزائري كأغلب التشريعات لا يقدم حلا لهذه المسألة وما نجده على مستوى العمل القضائي في الولايات المتحدة الأمريكية، وجود تضارب بين الأحكام القضائية بخصوص هذه المسألة ففيما إعتبرت بعض الأحكام أن جهاز الحاسوب بما يحتويه من ملفات ومعلومات

(1)أنظر في هذا المعني د.خالد ممدوح إبراهيم، المرجع السابق، 221.

(2)شيماء عبد الغني محمد عطاء الله،المرجع السابق. ص290.

صندوقا واحدا ولا يستوجب تفتيشه إلا إذنا واحدا فقط، إعتبرت على خلاف ذلك أحكام أخرى أن كل ملف في الحاسوب يتطلب إذنا خاصا لتفتيشه، مسببة حكمها على أساس أن الكومبيوتر يحتوي على الكثير من الملفات، و إذا كان أجيز لضابط الشرطة القضائية فتح الملفات الأخرى الموجودة داخل جهاز الحاسوب فإن ذلك سوف يؤدي بالفعل إلى الإعتداء على الحياة الخاصة التي يتمتع بها الفرد[1].

ومن الدول التي نصت تشريعاتها على ضرورة تحديد مجال الإذن بالتفتيش الولايات المتحدة الأمريكية وكندا حيث نصتا على أن يكون إذن التفتيش متضمنا:

- البحث عن أدلة متحصلة من كيان الحاسب المنطقي والتي يدخل فيها برامج التطبيق ونظم التشغيل.
- البيانات المستخدمة بواسطة برنامج الكومبيوتر.
- السجلات التي تثبت إستخدام الأنظمة الآلية لمعالجة البيانات .
- السجلات المستخدمة في عملية الولوج في النظام الآلي لمعالجة البيانات.

ثانيا: ضبط الدليل الرقمي: إن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها أثناءه فالضبط إذن هو غاية التفتيش القريبة والأثر المباشر الذي يسفر عنه الإجراء.

والأساس القانوني للضبط هو العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق والتي تفيد في كشف الحقيقة ما كان منها ضد المشتبه فيه أو ما كان في مصلحته.

ولقد تعودت جهات التحقيق في الجرائم التقليدية أن يقع الضبط على الأشياء المادية فقط بوصفها أدلة مادية للجريمة التي يجري التفتيش بشأنها، لكن في مجال الجرائم المعلوماتية الطبيعية العلمية المعقدة للدليل الرقمي الذي يوجب التفتيش عنه وضبطه لإثبات هذا النوع من الجرائم ليس كالدليل التقليدي، فالبيئة الإفتراضية لا تنتج سكينا أو سلاحاناريا وإنما تنتج نبضات رقمية تشكل قيمة وجوهر الدليل الرقمي فهل يصلح هذا النوع من الدليل لأن يكون محلا للضبط،وما هي الإجراءات المتبعة في ذلك؟

([1]) مشار اليه لدى رشيدة بوكر، مرجع سابق ،ص412.

1/مدى صلاحية ضبط أدلة الجرائم المعلوماتية:غني عن البيان أن الضبط هو وضع اليد على شيء يتصل بالجريمة ويفيد في كشف الحقيقة عنها وعن مرتكبها،[1]وهو كما سبق القول لا يرد إلا على الأشياء المادي، وعلى هذا الأساس فإن ضبط المكونات المادية للحاسوب لا يثير مشاكل في الفقه المقارن ولا يوجد خلاف بين فقهاء القانون في إمكانية ضبط هذه المكونات[2]بل حتى إمكانية ضبط الحاسوب بشكل كامل لتأكيد الإحتفاظ بالدليل إذا كان مشغل الجهاز غير متعاون مع جهات التحقيق.[3]أما بالنسبة لمكونات الحاسوب المعنوية فإن المسألة تحتاج إلى وقفة من أجل البحثفيها بشكل دقيق .

لقد إختلفت التشريعات الإجرائية والإتجاهات الفقهية حول مسألة ضبط الأشياء المعنوية والكيانات المنطقية والتي لا تصلح بطبيعتها محلا لوضع اليد وهي مجردة من دعامتها المادية المثبتة عليها، وإنقسمت في ذلك إلى إتجاهين:

الإتجاه الأول: يرى أصحابه أنه لا يمكن تصور إجراء الضبط على الكيانات المنطقية للحاسوب لإنتفاء الكيان المادي عنها، وبالتالي عدم صلاحية البيانات المخزنة آليا لأن تكون محلا للضبط بالكيفية المنصوص عليها بموجب النصوص التقليدية لإنتفاء الطابع المادي عن هذه البيانات في حال تجردها عن الدعامة المادية،[4]ومن التشريعات التي أخذت بهذا الإتجاه قانون الإجراءات الجنائية الألماني[5]

الإتجاه الثاني: يرى أنصار هذا الإتجاه أن المعطيات المخزنة آليا كونها مجردة عن الدعامة المادية التي تحويها لا يوجد ما يمنع من صلاحيتها بهذه الصورة لأن تكون محلا للضبط المنصوص عليه بمقتضى النصوص التقليدية مستندين إلى أن الغاية من التفتيش هو ضبط الأدلة التي تفيد في كشف الحقيقة وبالتالي يمتد هذا المفهوم ليشمل البيانات الإلكترونية بمختلف أشكالها.

([1])خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الأنترنات.دار الثقافة للنشر و التوزيع .الأردن 2011ص170.

([2])هاشم محمد فريد رستم. الجوانب الإجرائية للجريمة المعلوماتية، دراسة مقارنة مكتبة الآلات الحديثة أسيوط 1994، ص93.

([3])عفيفي كامل عفيفي.جرائم الكومبيوتر وحقوق المؤلف والمصفات الفنية ودور الشرطة والقانون دراسة مقارنة. منشأة المعارف الإسكندرية، ص353.

([4])عفيفي المرجع السابق، ص358.

([5])يرى أصحاب هذا الإتجاه أن يُصار إلى التدخل التشريعي لتوسيع دائرة الأشياء التي يمكن أن يرد عليها الضبط لتشمل بجانب الأشياء المادية البيانات الإلكترونية بكافة أنواعها وأنماطها المحوسبة.

وفي الجزائر فقد تدخل المشرع الجزائري بموجب القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، أين إستحدث المادة 06 التي تنص على أنه" عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفق القواعد المقررة في قانون الإجراءات الجزائية**...**" وإلى جانب الشرع الجزائري نجد المشرع الفرنسي قام بإدخال تعديل على قانون الإجراءات الجزائية بموجب قانون الأمن الداخلي 2003/239 أين إستحدث الفقرة الثالثة من المادة 57 التي تنص على المعطيات التي يتم بلوغها في ظل الشروط المنصوص عليها في المادة السابقة يتعين نسخها على دعامات التخزين المعلوماتية ويتم تحريزها في أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون"[(1)]

والسؤال المطروح هنا ما هي الأدلة التي يتم ضبطها في مجال إثبات الجريمة المعلوماتية؟

1.1/أنواع الأدلة محل الضبط في الجرائم المعلوماتية: إن الغاية من التفتيش هو صبط شيء يتعلق بالجريمة ويفيد التحقيق الجاري بشأنها سواء أكان هذا الشيء أدوات إستعملت في إرتكاب الجريمة أو شيئا نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة.[(2)]

والضبط في مجال الجرائم الإلكترونية يتصل بضبط المكونات المادية لأنظمة الحاسوب، ضبط المكونات المعنوية والبرمجيات، وكذا ضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط الحواسيب وما يتصل بها[(3)]

وعلى هذا الأساس فإن من الأشياء التي يتم ضبطها والتحفظ عليها في الجرائم المعلوماتية والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم:

([1])لقد كان هذا التعديل إستجابة لإتفاقية بودابست لعام 2001 التي نصت على ضبط الدليل الرقمي في الفقرة الثالثة من المادة 19 من القسم الرابع منها بإعتبارها أنه من سلطة كل دولة طرف أن تتخذ الإجراءات التالية:

أن تضبط نظام الكومبيوتر أو جزء منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكومبيوتر وأن تحافظ على سلامة تلك المعلومات المخزنة.

([2])عوض محمد المبادئ العامة في قانون الإجراءات الجنائية،الجزء الاول دار المطبوعات الجامعية. ص281.

([3])عيادالحلبي، المرجع السابق.ص169.

- ضبط جهاز الكومبيوتر وملحقاته:" ذلك أن ضبطه أمر مهم جدا للقول بأن الجريمة الواقعة هي جريمة معلوماتية وأنها مرتبطة بالمكان والشخص الحائز على الجهاز.[1]ولأجهزة الكومبيوتر أنواع مختلفة الأمر الذي يتطلب في ضابط الشرطة القضائية المعرفة الكافية التي تؤهله للتعامل معه والتعرف على مواصفاته بسرعة.

-ضبط المعدات المستعملة في شبكة الأنترنات وأهمها المودم (Modem) وهي الوسيلة التي تمكن أجهزة الكومبيوتر من الإتصال ببعضها البعض عبر خطوط الهاتف.

- وسائط التخزين المتحركة كالأقراص المدمجة (أقراص الليزر) والأقراص المرنة والأشرطة المغناطيسية.

- ضبط البرمجيات Softwareفإذا كان الدليل الرقمي ينشأ بإستخدام برنامج خاص فإن ضبط الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.

- ضبط البريد الإلكتروني والذي يحتوي على برامج متخصصة لكتابة وإرسال وإستعراض وتخزين الرسائل الإلكترونية،وهذه الرسائل لا يختلف التعامل معها عن التعامل مع الرسالة الورقية،إذ بمقدور المستخدم أن يطرحها جانبا أو يرد عليها أو ينقلها إلى شخص آخر أو يحفظ بها في ملف خاص، لذلك فالمحقق الذي يريد ضبط الرسائل الإلكترونية (boitte Email) الخاص به ثم يشغل برامج البريد الإلكتروني في جهاز حاسوبه ثم مراجعة قائمة الرسائل ليلتقط من بينها الرسالة المطلوبة.

2.1/الصعوبات التي تواجه المحقق أثناء عملية الضبط:إن عملية ضبط البيانات المعالجة آليا تواجهها عدة صعوبات أهمها:

-ضخامة البيانات التي من الواجب فحصها من قبل المحقق وذلك نتيجة حجم الشبكة التي تحتوي على هذه البيانات، الأمر الذي يتطلب من الخبرة الفنية ما يلزم لتحديد البيانات التي تصلح كأدلة جنائية من عدمه[2]

[1]خالد ممدوح إبراهيم،المرجع السابق، ص275

[2]عفيفي كامل عفيفي،المرجع السابق،355.

- قد يحتوي النظام المعلوماتي أو الشبكة المعلوماتية على عناصر لا يمكن فصلها ومع ذلك يتعين ضبطها، لأنها تتضمن عناصر الإثبات فيلزم بالضرورة ضبط النظام أو الشبكة كلها وهو الأمر الذي قد يترتب عليه التوقف عن العمل في المشروعات صاحبة النظام،[1] لذلك فإنه يتعين في هذه الحالة إعمال مبدأ التناسب والذي يقصد به إقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة ولها علاقة بالجريمة[2]

- كما أنه قد توجد هذه البيانات والمعطيات في شبكات وأجهزة تابعة لدولة أجنبية مما يستدعي تعاونها مع جهات التحقيق الوطنية.

- وإذا كانت عملية الضبط لهذه الوسائل التقنية تتم في الأنظمة المعلوماتية الكبيرة أو الشبكات الكبيرة فقد يؤدي إجراء الضبط إلى عزل النظام المعلوماتي بالكامل عن دائرته لمدة زمنية قد تطول أو تقصر، مما قد يتسبب في إلحاق أضرار بالجهة المستخدمة بالنظام بالإضافة إلى عدم إبداء مستخدمي الأنظمة المعلوماتية الإستعداد للتعاون الكامل والفعال مع سلطات التحقيق لما قد يعنيه إجراء الضبط بالنسبة لها مساسا بالسرية.

-كما أن الضبط في مجال المعلوماتية قد يمثل أحيانا إعتداء على حقوق الغير أو على حرمة حياتهم الخاصة مما يستوجب إتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات.[3]

ومن الصعوبات كذلك التي تعيق الوصول إلى ضبط الدليل الرقمي تلك الأحزمة الأمنية المفروضة من قبل مستخدم النظام حول البيانات التي يحويها هذا النظام، و مما يزيد من صعوبة الأمر على المحقق الجنائي عدم معرفته لكلمات السر أو شفرات المرور أو شفرات ترميز البيانات وقد لا يبدي المشتبه فيه تعاونه في الكشف عن هذه الشفرات لجهات التحقيق.

2/إجراءات ضبط الدليل الرقمي:يصعب إقامة الدليل على الجرائم التى تقع على العمليات الإلكترونية المختلفة وذلك بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة لأن محل تلك الجرائم كما عرفنا سابقا هو جوانب معنوية تتعلق بالمعالجة الآلية للمعطيات والتي تكون في هيأة

([1])شيماء عبد الغني، المرجع السابق،ص358.

([2])في هذا الصدد قضت المحكمة الفدرالية الألمانية بإلغاء قرار الضبط الذي ورد على 220 قرص صلب بالإضافة إلى الوحدة المركزية وذلك على سند مخالفة مبدأ التناسب.

([3]) أحمد أبو العلا عقيدة، المرجع السابق ص39.

رموز ونبضات مخزنة على وسائط تخزين ممغنطة لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحواسيب التي تحفظها، لأجل ذلك فإن القواعد التقليدية في الإثبات لا تكف لضبط مثل هذه البيانات .

لذلك فإن طريقة ضبط المعلومات المعاجة آليا تختلف عما هي عليه عند ضبط المكونات المحسوسة كالأقراص المرنة، المودم، والخادم...

ومن خلال دراستنا للقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها نجد أن المشرع وضع طريقتين لضبط الأدلة الرقمية، الأولى وتكون عن طريق نسخ المعطيات محل البحث على دعامة تخزين إلكترونية تكون هذه الأخيرة قابلة لحجزها ووضعها في أحراز حسب ما هو مقرر في قواعد تحريز الدليل المنصوص علها في قانون الإجراءات الجزائية، و الطريقة الثانية تكون باستعمال التقنيات المناسبة لمنع الاشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول الى المعطيات التي تحويها هذه المنظومة أو القيام بنسخها ويكون ذلك في حالة ما إذا استحال لأسباب تقنية ضبط هذه المعطيلت وفق الطريقة الاولى.

وإن كان الدليل الرقمي يخضع في ضبطه إلى قواعد تحريز الأدلة الجنائية عموما إلا أنه ونظرا إلى الطبيعة الخاصة له فإن عملية ضبطه وتحريزه تحتاج إإى بعض الإجراءات الخاصة لحمايته فنيا و الحفاظ عليه وصيانته من إمكانية العبث به، وهو مانوه عليه المشرع في المادة السادسة الفقرة الثالثة من القانون 04/09 حينما أوجب على السلطات التي تقوم بعملية ضبط الدليل الرقمي أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، وأن لا يؤدي إستعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات. ومن هذه الإجراءات الخاصة في هذا الاطار نذكر على سبيل المثال :

- أخذ نسخة احتياطية عن المعطيات و العمل عليها لضمان عدم المساس بالدليل الأصلي.
- عدم تنفيذ برامج على الحاسوب مسرح الجريمة خوفا من إتلاف الأدلة الموجودة عليه أو محو الذاكرة أو الملفات وعدم السماح للمشتبه به بالتعامل مع الحاسوب.
- ضبط الدعائم الأصلية للمعلومات وعدم الإقتصار على ضبط نسخها
- عدم ثني القرص لأن ذلك يؤدي إلى تلفه وفقدانه للمعلومات المسجلة عليه

- عدم تعريض الأقراص و الأشرطة الممغنطة لدرجات حرارة عالية و لا إلى الرطوبة .

وفي هذا الاطار بالذات نجد الهيأة الدولية لدليل الحاسب الآلي (IOCE) Organzation on computer evedenceInternational وضعت عدة ضوابط لعملية ضبط الدليل الرقمي منها ألا تكون الإجراءات المتخذة في تحريز الدليل الرقمي سببا في تغيير طبيعة هذا الدليل وأن تكون جميغ الأنشطة المتعلقة بتحريز الوثائق الرقمية أو الدخول إليها أو نقلها موثقة توثيقا كاملا مع المحافظة عليها وتوفيرها للمراجعة، وهو الأمر الذي أوردته كذلك الفقرة الثالثة من المادة 19 من الإتفاقية الأروبية للجريمة المعلوماتية.

الفرع الثاني: الخبرة في إثبات الجرائم المعلوماتية:

لقد ترتب عن التطور التقني في نظم المعالجة الآلية إلى تغيير كبير في المفاهيم السائدة حول الدليل، وقاد مثل هذا القول في الحقيقة إلى تعاظم دور الإثبات العلمي وإعلان إنضمام الخبرة التقنية إلى عالم الخبرة القضائية، ذلك أن إشتقاق الأدلة الرقمية المطلوبة في إثبات الجرائم المعلوماتية وكشف أنماطها أمر يضطلع به الخبراء المتخصصون في هذا المجال.

ولا يمكن التصور أن يرفض القاضي اللجوء إلى ندب خبير في قضايا تقنية المعلومات، إذ هي قضايا فنية تتطلب خبرة خاصة، ويكون حكمه مجانبا للمنطق العلمي ومعيبا إذا لم يستند إلى الخبرة التقنية في هذا المجال(1)تحقيقا لمبدأ هام هو مبدأ التخصص، وإذا كانت الخبرة التقنية في مجال التعاون القضائي تعد أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات والأنترنات خاصة إزاء نقص المعرفة لدى القانونيين بظاهرة تقنية المعلومات، فهل يعني هذا تعرض مبدأ "القاضي خبير الخبراء لهزات عنيفة إزاء التزايد المتواصل لمبدأ التفاعل القانوني مع ظاهرة البيئة الرقمية التي تقع في إختصاص آخر غير الجوانب النظرية القانونية التي لا تسمح ثقافة القاضي المبنية على معايير الدراسات القانونية من التفاعل معها.

أولا: القواعد القانونية التي تحكم الخبرة القضائية في مجال الجرائم المعلوماتية:الخبرة هي إجراء يستهدف إستخدام قدرات شخص الفنية والعلمية والتي لا تتوافر لدى رجل القضاء أو المحقق من أجل الكشف عن دليل يفيد في معرفة الحقيقة بشأن وقوع الجريمة.

وقد عرفها البعضبأنها الإستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته على نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه.(2)

والخبير هو كل شخص لديه دراية خاصة بمسألة من المسائل قد يستدعي التحقيق فحصها ويستلزم ذلك كفاء خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه، فيمكنه أن يستعين

(1)عادل عزام سقف الحيط،المرجع السابق ص273.

(2)ومن أهم التعريفات التي وردت بخصوص الخبرة القضائية أنها عبارة عن إجراءات من إجراءات التحقيق يعهد به القاضي إلى شخص مختص ينعت بالخبير وتتعلق بواقعة يستلزم بحثها أو تقديرها إبداء رأي يتعلق بها علما أو فنا لا يتوافر في الشخص العادي ليقدم له بيانا أو رأيا فنيا لا يستطيع المحقق الوصول إليه وحده.

بالخبير كما هو الحال مثلا في تقرير الصفة التشريحية في جرائم القتل أو تحليل المادة المطعومة في جرائم التسمم أو فحص خطوط الكتابة في جريمة التزوير.[1]

1/ أهمية الخبرة في البحث عن الدليل الرقمي:تكمن أهمية الخبرة في أنها تنير الطريق لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجزائية، لذلك فقد إهتم المشرع الجزائري بتنظيم أعمال الخبرة من المواد 143 إلى 156 من قانون الإجراءات الجزائية وإعتبارها من إجراءات البحث عن الدليل حيث نصت المادة 143 أنه لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما من تلقاء نفسها أو بناء على طلب من النيابة العامة و إما بطلب من الخصوم.

وإذا كانت الإستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر واجب على جهات التحقيق، فهي أوجب في مجال إستخلاص الدليل الرقمي لإثبات الجرائم المعلوماتية حيث تتعلق بمسائل فنية آية في التعقيد، يصعب على المحقق أن يشق طريقة فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات،[2] ومنذ ظهور الجرائم المعلوماتية فإن الضبطية القضائية وسلطات التحقيق عموما تستعين بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي والمنظومات المعلوماتية وذلك بغرض كشف غموض الجريمة وتجميع أدلتها والتحفظ عليها، أو مساعدة المحقق في إجلاء جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق ويلاحظ أن نجاح الإستدلالات وأعمال التحقيق في هذه الجرائم يكون مرهنا بكفاءة وتخصص هؤلاء الخبراء، فإجرام الذكاء والفن لا يكشفه ولا يفله إلا ذكاء وفن مماثلين،[3]وتبرز أهمية الإستعانة بالخبير في مجال الجرائم المعلوماتية عند غيابه فقد تعجز الضبطية في كشف غموض الجريمة لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي إرتكبت

---

(1)عبد الناصر محمد محمودفرغلي و محمد عبيد سيف سعيد الغافري،المرجع السابق. ص24.

(2)علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي،ورقة عمل للمؤتمر العلمي الاول حول الجوانب القانونية و الامنية للعمليات الالكترونيو دبي 2003 منشور على موقع: www.arablawinfo.com بدون ترقيم.

(3)محمد أبو العلاء عقيدة، المرجع السابق ص6،

بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل أو الإهمال عند التعامل معه.(1)

ولعل هذه الأهمية للخبرة في مجال التحقيق في الجريمة المعلوماتية جعل بعض التشريعات لا تكتف بالنصوص التقليدية التي تنظم الخبرة وعمدت على إدراج نصوص قانونية خاصة تنظم الخبرة في هذا المجال، ومنها المشرع البلجيكي بموجب القانون الصادر في 2000/11/23 حيث نصت المادة 88 منه أنه يجوز للقاضي والشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام وكيفية الدخول فيه أو الدخول للبيانات المخزنة أو المعالجة أو المنقولة بواسطته، ويعطي القانون لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق".

والمشرع الجزائري لم يتخلف عن هذه التشريعات حينما أشار في المادة 05 الفقرة الأخيرة من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها أنه يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

2/شروط صحة الخبرة ومدى حجيتها:نظرا للأهمية البالغة للخبرة والدور الذي تلعبه في عملية الإثبات في المجال الجنائي، فقد حرصت معظم التشريعات على تنظيم الخبرة ووضع شروط وضوابط لها. وبشكل عام فإن الفقه الجنائي يقدر أن الخبرة تستدعي توافر ركنين أساسين هما: الركن الشكلي والركن الموضوعي، وإذا كان هذا الأخير مقدورا له قدرا من الحرية العلمية ويكون الخبير فيه مستخدما لأدواته العلمية والعملية التي بمقتضاها ينطلق إلى وضع الإجابة على المعضلة الفنية محل سؤال جهات التحقيق، فإن الركن الشكلي فيها يمثل التخصص والعلم الذي إكتسبه الخبير، إذ يشترط في الخبير حقيقة الجمع بين العلم ذي الإختصاص والخبرة العلمية، فلا يكفي فقط كفاءة علمية عالية في مجال التخصص بل يضاف إليها سنوات من أعمال الخبرة في المجال،

(1)فقد حدث أن طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلي للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة فحدث نتيجة لذلك أن تسببت دوائر الشرطة بدون قصد في إتلاف ما كان قد تم من الملفات والبرامج.أنظر للتفصل أكثر د.هشام رستم الجوانب الإجرائية للجرائم المعلوماتية 1994، المرجع السابق. ص29.

حيث سار التقليد القضائي في هذا الإطار على ضرورة اللجوء إلى الخبرة المتوافر فيها هذان الركنان.

ومن الشروط التي درجت أغلب التشريعات على تحديدها منها ما يتعلق بالخبير ومنها ما يتعلق بتقرير الخبرة. فأما ما يتعلق بالخبير فأنه يشترط:

*إختياره من قائمة الخبراء المحددة أسماؤهم ضمن الجدول المعد مسبقا، وقد نصت المادة 144 من قانون الإجراءات الجزائية على ذلك بقولها:" يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد إستطلاع رأي النيابة العامة".وإذا لم يتضمن الجدول من الخبراء المتخصصين في مجال الخبرة فإنه يجوز لجهات التحقيق بصفة إستثنائية إختيار خبراء ليسوا مقيدين في الجدول .

وفي الحقيقة فإن الإستعانة بالخبراء وفق المنهج التقليدي في الإجراءات الجزائية يرتبط بمنطق تقليدي، يجب أن يتسع صدر المشرع الإجرائي بصددها بما يسمح بتجاوزها في إطار الجرائم المعلوماتية، ذلك أنه فضلا عن قاعدة أنه ليس في القانون ما يمنع جهات التحقيق من ندب خبراء من غير المقيدين بالجدول فإن هذا التوجه يجب أن يتم تطويره لكي يمكن الإستعانة بخبراء في العالم الإفتراضي إلى أبعد من النطاق الإقليمي ممثلا في الحدود المادية للدول بحيث يمكن أن يكون هؤلاء الخبراء من خارج الدولة وهو أمر تسمح به مقومات العالم الإفتراضي بإعتباره بيئة إتصالية رقمية عالمية.(1)

*حلف اليمين القانونية، إذ يجب لصحة عمل الخبير أداء اليمين القانونية وذلك لحمله على الصدق والأمانة في عمله وبث الطمأنينة في آرائه التي يقدمها سواء بالنسبة لتقدير القاضي أو لثقة بقية أطراف الدعوى، ولا يغني عن هذا الإجراء أي ضمانة أخرى من الضمانات، وقد أوجب المشرع الجزائري بنص المادة 145 من قانون الإجراءات الجزائية أن يحلف الخبير اليمين القانونية قبل أداء مهمته غير أنه إذا كان الخبير المعين مقيدا في الجدول فلا يلزم أن يجدد حلفه لليمين مرة أخرى.

وأما الشروط المتعلقة بتقرير الخبرة فإن الخبير بعد إنتهائه من أبحاثه وفحوصاته يعد تقريرا يضمنه خلاصة ما توصل إليه من نتائج، بعد تطبيق الأسس والقواعد العلمية الفنية على المسألة محل البحث.وإن كان المشرع لم يوجب إتباع شكل معين في تقرير الخبرة فقد يكون شفويا وقد يكون

---

(1)ممدوح إبراهيم، المرجع السابق ص292،.

كتابيا وفقا لما تحدده طبيعة المأمورية.[1]لكن الواقع العملي أثبت أن ما يتم في الغالب الأعم هو أن يطلب من الخبير إيداع تقريره كتابة، سيما إذا ما كانت المسألة موضوع الخبرة تتطلب إجراء أبحاث وتجارب وفحوصات علمية وعملية ومعملية. وغالبا ما يرفق الخبير بالتقرير ملحقا إيضاحيا بالصور حتى يسهل على جهة التحقيق فهم الخبرة وعلى جهة الحكم تكوين عقيدتها وإقتناعها الذاتي بالدليل.

وإذا كان الحال كذلك بالنسبة لموضوعات الخبرة التقليدية فإن أهمية إعداد تقارير فنية مكتوبة وملاحق توضيحية مصورة تصبح حتمية في حالة الجرائم المعلوماتية، حيث يقتضي الأمر عرض وتوضيح وتحليل الدليل الجنائي الرقمي وكيفية إشتقاقه وإستخلاصه.

ويشترط أيضا فيما يتعلق بتقرير الخبرة أن يقوم الخبير بإيداع تقرير خبرته خلال المدة المحددة له في أمر أو حكم الندب، فإن لم يودع تقريره خلال هذه المدة جاز للقاضي إستبداله بغيره ما لم يقدم الخبير طلبا بتمديد هذه المهلة وذلك نظرا لما تتسم به الإجراءات الجزائية من طابع السرعة سيما إذا تعلق الأمر بالجريمة المعلوماتية.

ثانيا: القواعد الفنية التي تحكم عمل الخبير في مجال الجرائم المعلوماتية:تتنوع الوسائل الإلكترونية والأجهزة التي تستخدم نظام الحاسبات الآلية، كما تتنوع شبكات الإتصال بينها وتتمايز خصائصها الفنية فتندرج تحت تخصصات فنية وعلمية دقيقة مما يستوجب والحال كذلك أن يتوافر لدى الخبير الإمكانيات والقدرات العلمية والفنية في مجال التخصص، وعلى جهات التحقيق أن تدقق عند إختيارها للخبير وتتيقن من هذه المسألة.

كما أن عملية تجميع الدليل الرقمي تعد من أصعب الأمور التي تواجه الخبير التقني، لذلك كان لزاما عليه إتباع خطوات وأساليب علمية تتناسب مع البيئة التي يتواجد بها هذا النوع من الدليل.

1/متطلبات أعمال الخبرة في مجال الجريمة المعلوماتية:إنه بالنظر إلى الطبيعة الفنية والعلمية للخبرة في مجال الجريمة المعلوماتية فإنه ينبغي للخبير الإلمام بالموضوعات الآتية:[2]

(1)عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، المرجع السابق.ص27،

(2)هشام رستم، المرجع السابق.ص142-143،

- الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور أو السر ورموز التشفير.

- طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

- القدرة على أداء المهام دون أن يترتب على ذلك إعطاب أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية.

- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة.

- بالإضافة إلى ضرورة إلمام الخبير أيضا[1]بنظم الحاسب الآلي بمكوناته المادية والبرامجية.

- معرفته لوسائل وطرق فحص نظام الحاسب الآلي كبرامج كشف وإزالة للفيروسات وبرامج إسترجاع البيانات والمعلومات وإصلاح التالف وإظهار المخفي منها.

- معرفته لوسائل نسخ البرامج والملفات وعمل نسخ من القرص الصلب طبق الأصل.

- معرفته لكيفية الربط بين الدليل المادي والدليل الرقمي في الوقائع محل البحث.

ولا ينجح الخبير المعلوماتي في أدائه لمهامه المنوطة به وإتمامه للمأمورية المكلف بها إن لم يكن لديه هذا القدر من المتطلبات الفنية.

فالخبرة في الجرائم المعلوماتية تساعد في النهاية على:

- الكشف عن الدليل الرقمي.

- إجراء الإختبارات التكنولوجية على الدليل الرقمي للتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنفاذ القانون.

- تحديد الخصائص الفريدة للدليل الرقمي.

- إصلاح الدليل الرقمي وإعادة تجميعه من المكونات المادية للكومبيوتر.

- عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية إستخلاص الدليل.

([1])عبد الناصر محمد محمود فرغلي ود محمد عبيد سيف سعيد المسماري، المرجع السابق،ص33.

- جمع الآثار المعلوماتية الرقمية التي تكون قد تبدلت خلال الشبكة المعلوماتية.

2/الأساليب الفنية في عمل الخبير المعلوماتي في إكتشاف الدليل الرقمي:للخبير المعلوماتي في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها، وهو في إطار القيام بعمله له أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها لها مسببا بشكل منطقي[(1)]

ويعتمد عمل الخبير المعلوماتي في سبيل تحري الحقيقة في مجال الجرائم المعلوماتية على جمع مجموعة من الأدلة الرقمية وتحصيلها من خوادم المواقع (Les serveurs)ومن جهاز المعتدي بعد التوصل إلى تحديده، ثم يقوم بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها، ومن ثم التوصل في النهاية إلى معرفة بروتكول الأنترنات (IP) للحاسوب الذي صدرت منه الرسائل والنبضات الإلكترونية.

ويرى بعض المتخصصين أن عمل الخبير المعلوماتي في إشتقاق وتجميع الأدلة الرقمية يتم عبر ثلاث مراحل:

المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة من خلال تتبع الحاسبات الخادمة التي دخل منها المجرم المعلوماتي ومحاولة إيجاد أثر له.

المرحلة الثانية: مرحلة المراقبة ويتم ذلك بطرق مختلفة أهمها إستخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع.

المرحلة الثالثة: فحص النظام المعلوماتي المشتبه فيه بعد ضبطه من طرف جهات التحقيق بمكوناته المادية والمعنوية لإشتقاقالدليل وتقديمه لجهات التحقيق وتقرير مدى وقوع الجريمة بإستخدام النظام المضبوط من عدمه.

وقد وضعت وزراة العدل الأمريكية إطارا عمليا يحدد خطوات أساسية لجمع الأدلة الرقمية ثم فحصها ومن ثم تحليلها وأخيرا كتابة النتائج المتوصل إليها في تقرير، ويمكن إيجاز هذه الخطوات في المراحل التالية:

-خطوات ما قبل التشغيل والفحص:

*التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدون عليها.

([1])خالد ممدوح إبراهيم، المرجع السابق،ص301.

*التأكد من صلاحية وحدات نظام التشغيل.

*تسجيل معطيات وحدات المكونات المضبوطة.

- خطوات التشغيل الفحص:

*إستكمال تسجيل باقي معطيات الوحدات من خلال قراءات الجهاز.

*عمل نسخة من كل وسائط التخزين المضبوطة وعلى رأسها القرص الصلب لإجراء عملية الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير سواء عن سوء الإستخدام أو لوجود فيروسات أو قنابل برمجية.

*تحديد أنواع وأسماء المجموعات البرامجيةكبرامج النظام (برامج التشغيل)، برامج التطبيقات وبرامج الإتصالات، وما إذا كان هناك برامج أخرى ذات دلالة بموضوع الجريمة.

*إظهار الملفاة المخبأة والنصوص المخفية داخل الصور.

*إسترجاع الملفات التي تم محوها من الأصل وذلك بإستخدام أحد برامج إستعادة المعلومات وكذلك بالنسبة للملفات المعطلة أو التالفة.

*تخزين هذه الملفات أو المعطيات وعمل نسخ أخرى طبق الأصل من الأسطوانة أو القرص المحتوي لها ولفحصها عن طريق تطبيق الخطوات سالفة الذكر.

*إعداد قائمة يبجرد فيها الخبير كل الأدلة الرقمية التي تم الحصول عليها، مع إجراء مراجعة لكل صورة محتفظ بها في القرص الصلب لحاسوب آخر للتأكد من سلامة القائمة.

*تحويل الدليل الرقمي إلى هيأة مادية وذلك عن طريق طباعة الملفات أو تصوير محتواها أو وضعها في أي وعاء آخر حسب نوع المعطيات والمعلومات المكونة للدليل.[(1)]

وفضلا عما سبق فإن الخبير المعلوماتي وهو في إطار القيام بعمله له أن يستخدم العديد من الوسائل العلمية والبرمجيات التي تمكنه من إستخلاص الدليل الرقمي و تساعده في الوصول إلى المجرم المعلوماتي، وغالبا ما تكون هذه الوسائل أدوات فنية تستخدم في بنية نظام المعلومات.

ونذكر منها على سبيل المثال لا الحصر:

([1])عبد الناصر محمد محمود فرغلي و عبيد سيف سعيد المسماري، المرجع السابق، ص35،.

*بروتوكول الأنترنات(IP)وهو المسؤول عن تراسل حزم البيانات عبر شبكة الأنترنات وتوجيهها إلى أهدافها، وهو يوجد بكل جهاز مرتبط بالأنترنات ويتكون من أربعة أجزاء كل جزء يتكون من أربع خانات، حيث يشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات المرتبطة، والرابع يحدد الكومبيوتر الذي تم الإتصال منه،[1]مع ملاحظة أن عنوان IP قد يتغير في كل إتصال بشبكة الأنترنات.

*نظام البروكسي(PROXY): يعمل هذا النظام كوسيط بين الشبكة ومستخدميها بحيث يضمن مقدم الخدمة توفير خدمات الذاكرة الجاهزة، وتقوم فكره البروكسي على تلقي مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما ضمن الذاكرة الجاهزة، فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد تم تتزيلها من قبل فيقوم بإرسالها إلى المستخدم دون حاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يتم تتزيلها من قبل فيتم إرسال الطلب إلى الشبكة العالمية وهنا يستخدم البروكسي أحد عناوين IP. ومن أهم مزايا هذا النظام أن الذاكرة المتوفرة لديه يمكن أن تتحفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة.

*برنامج الدمج وفك الدمج(pkzip) ويستخدم هذا البرنامج لفك دمج البرامج، فقد يكون المجرم المعلوماتي قد قام بدمج برامجه فلا يمكن الإطلاع عليها إلا بعد فك الدمج.

*برنامج Visual route5.2 aوهو عبارة عن برنامج يلتقط أي عملية فحص ضد الشبكة فيقوم بتقديم أجوبة تبين المعلومان التي حدث فيها المسح والمناطق التي تم فيها الهجوم، وبعد معرفة عنوان IPإسم الجهة يرسم البرنامج خطا يوضح من خلاله مسار الهجوم بين مصدره والجهة التي إستهدفها الهجوم.

*برنامج معالجة الملفات: (Xtree Progold) وهو برنامج يمكن من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم والأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية.

([1])وتوجد أكثر من طريقة يمكن من خلالها معرفة عنوان IP الخاص بجهاز الحاسوب منها على سبيل المثال ما يستخدم في حالة العمل على نظام تشغيل Windous حيث يتم كتابة WINPCFG في أمر التشغيل ليظهر مرجع حوار بين فيه IP

*برنامج Hark Tracerv1.2وهو أحد برامج التتبع يتكون من شاشة رئيسية تقدم للمستخدم بيان شامل بعمليات الإختراق التي تعرض لها جهازه، يحتوي على تاريخ الواقعة وعنوان IP الذي تم من خلاله عملية الإختراق وإسم الدولة التي منها الإختراق وإسم الشركة المزودة لخدمة الأنترنات المستضيفة للمخترق ورقم المنفذ والبوابة الخاصة وبيانات الشبكة التي تتبعها الشركة المستضيفة للمخترق بما فيها أرقام هواتفها.

المطلب الثاني: القواعد الإجرائية الحديثة لإستخلاص الدليل الرقمي:

لم تسلم طرق الإثبات من تأثيرات ثورة المعلومات وتكنولوجيا الإتصالات، فالتناغم المطلوب تحقيقه دائما بين طبيعة الدليل وطبيعة الجريمة التي يولد منها ويصلح لإثباتها، أفرز إلى حيز الوجود طرقا إجرائية تتناسب والطبيعة التقنية للجريمة المعلوماتية وللدليل الرقمي، لكي يمكن عن طريقها الوصول إليه وإستخلاصه ونقصد بذلك تكريس تقنية المعلومات لجمع الدليل الرقمي.

ومن ضمن المقومات التشريعية التي أرساها المشرع الجزائري ضمن خطته في مكافحة الجريمة المعلوماتية، ما جاء به في القانون 22/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية(الأمر 155/66) من خلال إجرائي التسرب وإعتراض المراسلات، ثم من خلال القانون 04/09 إستحدث إجرائين آخرين وهما المراقبة الإلكترونية وحفظ المعطيات المتعلقة بحركة السير.

الفرع الأول: التسرب وإعتراض المراسلات

تعتبر الجريمة المعلوماتية من بين الجرائم التي يمكن فيها اللجوء إلى إجراء التسرب أو إعتراض المراسلات إذا اقتضت ذلك الضرورات التحري أو التحقيق بشأنها.

أولا:التســــــربلقد حدد المشرع الجزائري نطاق هذا الإجراء بالجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 5 من قانون الإجراءات الجزائية والتي من بينها الجرائم الماسة بأنظمة المعالجة الآلية المعطيات(1)

1/مفهوم التسرب وشروطه:لقد نظم المشرع هذا الإجراء في قانون الإجراءات الجزائية وفق ثمانية مواد من المادة 65 مكرر 11 إلى المادة 65 مكرر 18 تناول من خلالها تحديد مفهوم هذا الإجراء وشروطه وسنحاول تفصيل ذلك من خلال ما يلي:

(1)أنظرنص المادة 65 مكرر 5 و65مكرر 11.

1.1/مفهوم التسرب:إن التسرب من الناحية الأمنية هو تلك العملية المحضر لها والمنظمة، المراد من القيام بها التوغل داخل وسط لمعرفة حقيقته معرفة جيدة من خلال نشاطه البارز وكشف الخفي فيه، ويكون هذا الوسط محددا مسبقا بطبيعته والعمل من أجل الإستعلام عنه ومعرفة أدق التفاصيل فيه وخصوصياته وأسراره حسب تطلعات الجهات الأمنية وفائدة المصلحة،أما من الناحية القانونية فالمشرع الجزائري حدد المقصود بهذا الإجراء بموجب المادة 65 مكرر 12 على أنه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف[(1)]

ويلاحظ من خلال ما سبق ذكره أن التسرب عملية معقدة تتطلب أن يدخل العون المكلف بالعملية في إتصال بالأشخاص المشتبه فيهم ويربط معهم علاقات من أجل تحقيق الهدف النهائي من العملية، وتتطلب على الخصوص المشاركة المباشرة في نشاط الخلية الإجرامية التي تسرب إليها.

وعلى هدي ذلك فإن التسرب يرتكز على مبدئين:

المبدأ العام يستند على تقديم صورة على الوسط المراد التسرب فيه، ويستوجب ذلك معرفة عموميات عن هذا الوسط مع توثيق هذه المعطيات.

والمبدأ الخاص الذي يستند على تعميق التحري عن هذا الوسط ونشاطاته ومميزاته ووسائله وطبيعة الأشخاص المنتمين إليه، ليتم بعد ذلك دراسة الوظيفة العملياتية في هذا المجال بتوفير الوسائل البشرية والتقنية اللازمة.

2.1/شروط التسرب:إنه ومن أجل إنجاح عملية التسرب وتسهيل مهام الشخص المتسرب لبلوغ الهدف المرجو من هذا الإجراء بإعتباره ممارسة غير مألوفة للضابط أو عون الشرطة القضائية، وكذا لكون هذا الإجراء من أخطر الإجراءات إنتهاكا لحرمة الحياة الخاصة للمشتبه فيه، فقد أحاطه المشرع بجملة من الشروط يتعين مراعاتها عندما تقتضي ضرورات التحري والتحقيق اللجوء إليه.

([1])تكلم المشرع الفرنسي عن التسرب(Infiltration) في المواد 81/706 إلى 87/706 وكذا المادتين 7/694 و9/694من تعديل قانون الإجراءات الجزائية بموجب القانون 297/2007 المؤرخ في 2004/03/09.

1.2/الشروط الشكلية: تنحصر الشروط الشكلية لهذا الإجراء في الإذن وما يجب أن يتضمنه فلا يمكن بأي حال من الأحوال أن يباشر ظابط الشرطة القضائية عملية التسرب بمفرده دون أن يكون متحصلا على إذن بذلك من قبل الجهات القضائية المختصة، وهذا ما نصت عليه المادة 65 مكرر 11 من قانون الإجراءات الجزائية"**....**يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن**....** حسب الحالة بمباشرة عملية التسرب".

فالجهة المختصة بإصدار أو منح الإذن بالتسرب إما وكيل الجمهورية أو قاضي التحقيق ويجب أن يكون هذا الإذن مكتوبا وإلا كان الإجراء باطلا، وهذا ما نصت عليه المادة 65 مكرر 15 بقولها يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 مكتوبا تحت طائلة البطلان" وذلك لأن الأصل في العمل الإجرائي الكتابة، ومن جهة أخرى فإن الإذن يجب أن يتضمن مجموعة من الشروط يتوقف على تحديدها صحة الإجراء في حد ذاته كذكر هوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته، بالإضافة إلى تحديد المدة المطلوبة في عملية التسرب والتي يجب ألا تتجاوز أربعة أشهر ويمكن أن تجدد حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية، وفي نفس الوقت أجاز القانون للقاضي الذي أذن بهذا الإجراء أن يأمر في أي وقت يوقفه قبل إنقضاء المدة المحددة.

2.2/الشروط الموضوعية: يمكن إيجاز الشروط الموضوعية لعملية التسرب وفق الأحكام التي نظمها المشرع الجزائري في شرطين أساسين:

-الأول يتمثل في تحديد نوع الجريمة والتي يجب ألا تخرج عن الجرائم التي حددتها على سبيل الحصر المادة 65 مكرر 05 في سبعة أنواع وهي**:**" جرائم المخدرات، الجريمة المنظمة العابرة للوطنية، جرائم تبيض الأموال، الجرائم الإرهابية، جرائم الفساد، الجرائم المتعلقة بالتشريع الخاص بالصرف والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

- أما الشرط الموضوعي الثاني فهو أن يكون الإذن بالتسرب مسبباً،فمن خلال التسبيب تتبين العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن وكذا العناصر التي دفعت ضابط الشرطة القضائية للجوء إلى هذا الإجراء والتي تكون ضمن موضوع طلبه الإذن.

لذلك فكان لزاماً عند إصدار الإذن بالتسرب سواءا من طرف وكيل الجمهورية أو من طرف قاضي التحقيق إظهار جميع الأدلة بعد تقدير العناصر المعروضة عليه من طرف ضابط الشرطة القضائية.(1)

2/طرق التسرب في مجال الجريمة المعلوماتية: يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى العالم الإفتراضي وذلك بإختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو إشتراكه في محادثات غرف الدردشة أو حلقات الإتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما في ذلك أسماء أو صفات هيآت مستعارة ووهمية سعيا منه للإستفادة منهم حول كيفية إقتحام الهاكر للموقع.

ثانيا: إعتراض المراسلات السلكية واللاسلكية: إستحدث المشرع الجزائري بموجب القانون رقم 22/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية من خلال الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور، وقد ضمنه ستة مواد من المادة 65 مكرر إلى المادة 65 مكرر 10، وتناول من خلالها المقصود بهذا الإجراء وضمانات إستخدامه.

1/مفهوم إجراء إعتراض المراسلات السلكية واللاسلكيةوشروطه القانونية: إستحدث المشرع الجزائري هذا الإجراء بموجب القانون رقم 22/06 المؤرخ في ديسمبر سنة 2006المعدل و المتمم لقانون الإجراءات الجزائية

1.1/مفهوم إعتراض المراسلاتالسلكية و اللاسلكية: ورد في إجتماع لجنة الخبراء للبرلمان الأوروبي بسترازبورغ المؤرخ في 2006/20/06 حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية تعريفا لإجراء إعتراض المراسلات بأنها عملية مراقبة سرية المراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في إرتكاب الجرائم.(2)

---

(1)نصت المادة 65 مكرر 15 على أنه يجب أن يكون الإذن بمباشرة عملية التسرب....مسببا وذلك تحت طائلة البطلان".

(2)مشار له لدى لوجاني نور الدين أساليب البحث والتحري الخاصة وإجراءاتها وفقا لقانون 22/06 مداخلة في يوم دراسي حول علاقة النيابة بالشرطة القضائية "إحترام حقوق الإنسان ومكافحة الجريمة، وزارة الداخلية المديرية العامة للأمن الوطني منعقد يوم 2007/12/12 بإليزي ، ص8.

ومن خلال نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية نجد أن المشرع الجزائري يقصد بإعتراض المراسلات، إعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الإتصال السلكية واللاسلكية، وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع ،التخزين، الإستقبال والعرض.

وإلى جانب المشرع الجزائري نجد كذلك المشرع الفرنسي قد كرس هذه التقنية في المادة 100 من قانون الإجراءات الجزائية التي تنص على أنه في المواد الجنائية والمواد الجنحية إذا كانت العقوبة تفوق سنتين يمكن لقاضي التحقيق إذا دعت مقتضيات البحث والتحري أن يأمر بإعتراض وتسجيل ونقل المراسلات التي تتم عن طريق وسائل الإتصال"

ولقد حدد المشرع الفرنسي مفهوم المراسلات الخاصة التي تكون محلا للإعتراض من خلال المنشور المؤرخ في 1988/02/17 الذي إعتبر أنه تكون المراسلة خاصة إذا كانت الرسالة موجهة بصورة حصرية لشخص أو أشخاص طبيعيين أو معنويين محددين على وجه الخصوص"[1]بغض النظر عن الشكل الذي تكون عليه.

أما في القانون الجزائري نجد المادة 9-6 من القانون 03/2000 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات،اعتبرت أن مادة المراسلات هي كل إتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف الرسل نفسه أو بطلب منه، ولا تعتبر الكتب والجرائد والمجلات واليوميات كمادة مراسلات.

وبالتالي فحسب مفهوم هذه المادة فإن المراسلات الخاصة تصبح محصورة في الرسائل المكتوبة بالمفهوم التقليدي.

إلا أنه وبالرجوع إلى نص المادة 39 من الدستور الجزائري التي تنص على أن سرية المراسلات والإتصالات الخاصة بكل أشكالها مضمونة، وكذا نص المادة 303 من قانون العقوبات التي تعاقب كل من يفض أو يتلف رسائل أو مراسلات موجهة للغير، فإنه يمكن التوصل للقول أن المراسلات الخاصة تعني كل رسالة مكتوبة بأي شكل من الأشكال سواء ماديا أو إلكترونيا وسواء

---

[1]circulaire francaise du 17 février 1988 prise en application de larticle 43 de loi 86-1067 du 30 septemper 1986 relative a la liberté de comminication concernant le régime déclaratif aplicable a certains services de comanunication audivisuelle jorf du 09 mars 1988 p31-49.

كانت على دعامة ورقية أو رقمية، مرسلة بأي وسيلة لعدد معين ومحدد من المرسل إليهم، بإستثناء الكتب والمجلات والجرائد والحوليات التي لا تعتبر مراسلات خاصة.

وهذا ما يؤكده القانون 04/09 في المادة 02/الفقرة "و" في تعريفه للإتصالات الإلكترونية على أنها أن تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

وتختلف وتتنوع المراسلات عبر وسائل الإتصالات الإلكترونية والتي من أهمها التراسل عبر البريد الإلكتروني، فهذه التقنية تم إبتكارها ليتمكن مستخدموها من تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة ثم ترسل تلك الرسالة من بريد شخص إلى آخر عبر عنوان بريد إلكتروني دونما أي إبطاء.

ويتمتع البريد الإلكتروني بخدمة قائمة التراسل (Mailinglist) وهو نظام تراسل جماعي يمنح صلاحية بث رسالة إلى مجموعة من الأشخاص المسجلين في هذه القائمة، ويحتوي البريد الإلكتروني برامج متخصصة لكتابة الرسائل الإلكترونية وإرسالها وإستعراضهاوتخزنتها.

وقد إبتكرت نظم البريد الإلكتروني برامج تشفير خاصة لحماية خدمة البريد الإلكتروني من الإختراقات وضمان خصوصية محتوياتها.

وإذا كانت هذه المراسلات تتمتع بالخصوصية حمى المشرع سريتها بسن قوانين تعمل على توفير قدر كبير من الحماية الجزائية لها، إلا أن هذا الأمر ليس على إطلاقه فإذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فإنه يجوز إعتراض هذه المراسلات وكشف السرية عنها في سبيل البحث عن الدليل، وهو السند الشرعي المبرر لإباحة هذا الإجراء بسبب أنه يتضمن إعتداء جسيما على حرمة الحياة الخاصة وسرية الإتصالات، فيباح إستثناءا وفي حدود ضيقة وذلك للفائدة المنتظرة منه والتي تتعلق بإظهار الحقيقية وكشف الغموض عن الجريمة وضبط الجناة.(1)

وتجدر الإشارة في هذا الصدد أن المراسلات التي تصلح لإجراء إعتراضها يجب أن تتسم بالخصوصية، ولكي تكون كذلك يلزم أن يتوافر لديها عنصران أساسيان هما:

---

(1) محمد أبو العلاء عقيدة، مراقبة المحادثات التلفونية، دراسة مقارنةدار النهضة العربية 2008 ،ص192.

- عنصر موضوعي ويتعلق بموضوع ومضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي وسري أو خاص فيما تخبر به.

- وعنصر شخصي والمراد به إرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون الرسالة،[1]وهذا الأمر ذهبت إلى تأكيده المحكمة العليا بكندا بقولها أن الحالة الذهنية للمرسل هي الحاسمة في تحديد الصفة الخاصة أو العامة للإتصال، ونفس الإتجاه أخذته إحدى المحاكم في الولايات المتحدة الأمريكية حيث أشارت إلى أن خصوصية الرسائل الإلكترونية تعتمد بشكل كبير على طبيعة تكلم الرسائل وطبيعة مرسلها،[2]وعند توافر هذان العنصران في الرسالة فإنها تتصف بالمراسلة الخاصة التي لها خصوصيتها وسريتها المحمية قانونا ولا أهمية لشكل الرسالة أو طرق نقلها وتوصيلها إلى المرسل إليه.

2.1/الشروط والضمانات المقررة لإعتراض المراسلات السلكية و اللاسلكية: مما لاشك فيه أن أسلوب إعتراض المراسلات السلكية واللاسلكية دون علم أصحابها بقدر ما يفيد في كشف الحقيقة ويسهل إثبات كثير من الجرائم الغامضة كتلك المتعلقة بالجرائم المعلوماتية، فهو من جانب آخر يمثل إنتهاكا لحرمة الحياة الخاصة للأفراد وإعتداء على سرية مراسلاتهم وإتصالاتهم التي كفلتها الدساتير والتشريعات العقابية.[3]والمشرع الجزائري في هذا الصدد كما أعطى لسلطات التحقيق مكنة إعتراض المراسلات كأسلوب مستحدث للبحث عن الدليل يتماشى مع الأساليب المتطورة التي يلجأ إليها الجناة في تنفيذ جرائمهم وإخفاء أي أثر يدل عليهم، فمن ناحية أخرى لم يفتح الباب على مصرعيه في اللجوء إلى هذه الوسيلة بل أحاط إستخدامها بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية وتتمثل هذه الشروط في:

1.2/ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ: طبقا للمادة 05 مكرر من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء إعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة

([1])نشوى رأفت إبراهيم الحماية القانونية لخصوصية مراسلات البريد الإلكتروني، بحث مقدم في كلية الحقوق بجامعة المنصورة، ص04 .

([2])مشار إليه لدى د عمر محمد بن يونس، أشهر المبادئ المتعلقة بالأنترنات في القضاء الأمريكي دار النهضة العربية القاهرة 2004، ص582.

([3])الحماية على مستوى الدساتير أنظر المادة 39 من الدستور الجزائري التي تنص "...أن سرية المراسلات والإتصالات الخاصة بكل أشكالها محمية" والحماية على مستوى النصوص العقابية أنظر المادة 303 مكرر من قانون العقوبات الجزائري.

فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية هذا الإجراء.(1)

وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقدير فائدة إجراء الإعتراض وجديته وملاءمته لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا، مع ملاحظة أنه في فرنسا ومنذ صدور القانون 204/2004 المؤرخ في 2004/03/09 المعدل لقانون الإجراءات الجزائية أصبح حسب المادة 95/706 الإذن بإعتراض المراسلات من إختصاص قاضي الحريات والإحتباس بمنحه بناءا على طلب من وكيل الجمهورية إذا تعلق الأمر بالتحقيق في الجرائم المحددة حصرا بالمادة 706-73، وتخضع إجراءات الإعتراض لرقابته في أجل 15 يوم قابلة للتجديد بنفس الشروط في الشكل والأجل.

وقد نصت المادة 65 مكرر 09 على أن عملية تنفيذ إجراء إعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به وذلك من خلال قيام ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بإعداد محضرا عن كل عملية إعتراض للمراسلات وكذا عن عمليات وضع الترتيبات التقنية لهذا الغرض، ويذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات والإنتهاء منها.

2.2/تحديد طبيعة المراسلة ومدة الإعتراض: وهذا ما يفهم صراحة من نص المادة 65 مكرر 7 التي نصت على أنه يجب أن يتضمن الإذن بإعتراض المراسلات كل العناصر التي تسمح بالتعرف على الإتصالات أو المراسلات المطلوب إعتراضها، كما أن المشرع قد إستوجب أن لا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الإذن وفقا لمقتضيات التحري والتحقيق وهي نفس المدة التي حددها المشرع الفرنسي في المادة 100 من قانون الإجراءات الجزائية الفرنسي.

2/طرق إعتراض المراسلات الإلكترونية: يعتبر البريد الإلكتروني أهم وسيلة تقنية في مجال التراسل الإلكتروني ومن ثم فعملية الإعتراض تنصب عليه، ومن المعلوم أن كل رسالة إلكترونية يظهر فيها معلومات عامة مثل تاريخ إنشاء الرسالة وتاريخ تلقيها وكذا عنوان المرسل وعنوان

---

(1)تنص المادة 65 مكرر 05:" إذا إقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم.... أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية أن يأذن بإعتراض المراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاسلكية.... وفي حالة فتح تحقيق قضائي تتم العملية بناءا على إذن من قاضي التحقيق وتحت مراقبته المباشرة".

المرسل إليه، ولكن هذه المعلومات ليست كافية لمعرفة المرسل إذ بإمكان هذا الأخير إطلاق رسائله من صناديق بريد مسجلة بأسماء وهمية، كما أن هناك وسائل تتيح للمرسل أن يرسل رسالته دون أن يظهر فيها عنوان بريده الإلكتروني الصحيح لذلك لابد من الحصول على المزيد من المعلومات التي يمكن العثور عليها في حاشية رسائل البريد الإلكتروني والتي يطلق عليها مصطلح " Email Header" وهي أول خطوة للبدء بالتحري عن مرسل الرسالة الإلكترونية وهذه الحاشية لا تظهر بصورة مباشرة وإنما يتطلب الأمر من المستخدم إجراء بعض الخطوات للحصول عليها.[(1)]

والمعلومات التي تحتويها حاشية الرسالة(Email Header) هي عبارة عن معلومات تراكمية لمختلف الأجهزة الخادمة للبريد الإلكتروني التي مرت من خلالها الرسالة، فالمعتدي عندما يرسل رسالته تذهب تلك الرسالة إلى جهاز الحاسوب المركزي المملوك للجهة التي منحت له حساب البريد الإلكتروني، وذلك الجهاز يقوم فورا بإرسال الرسالة إلى الحاسوب المركزي الآخر المملوك للجهة التي منحت للمرسل إليه حساب البريد الإلكتروني، وهنا يقوم الجهاز الأخير بإرسال الرسالة إلى المرسل إليه ولهذا السبب نجد أن حاشية المعلومات ستتضمن أرقام"IP"مختلفة تمثل أرقام خاصة بكل الأجهزة التي مرت بها الرسالة، وعادة ما يظهر رقم IPالخاص بمرسل الرسالة أمام عبارة"xoriginating IP، وفي حالة عدم ظهور هذه العبارة فإن رقم IPالخاص لمرسل الرسالة يكون أمام آخر كلمة Received، وتعد في هذه المعلومة أساسية يمكن من خلالها الإستدلال على صاحب الرسالة ويصبح بعد ذلك من السهل الحصول على المزيد من المعلومات عن المرسل وذلك بإدخال رقم IPفي بعض المواقع التي تقوم بالكشف عن مصدر الرسالة والمكان الجغرافي الذي أرسلت منه وكذا مزود الخدمة الذي يتعامل معه مرسل الرسالة ويكون بذلك من السهل تماما إعتراض هذه المراسلات والإطلاع على محتواها دون علم مرسلها[(2)].

الفرع الثاني: المراقبة الإلكترونية وحفظ المعطيات:

سوف نتناول بالشرح إجراء المراقبة الإلكترونية فقط على إعتبار أنه سبق الحديث عن حفظ المعطيات.

([1])حول طرق إستخراج حاشية المعلومات في أشهر حسابات البريد الإلكتروني أنظر عادل عزام سقف الحيط،المرجع السابق. ص256.

([2]) أنظر مقال حول طريقة الكشف عن هوية مرسل البريد الإلكتروني، مجلة دليل الأنترنات. مجلة شهرية متخصصة العدد 109 السنة التاسعة 2009 مطبعة فيلمز الكويت.

إستحدث المشرع الجزائري إجراء المراقبة الالكترونية بموجب المادة الثالثة من القانون09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها حينما أجاز تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في إطار هذا النوع من الجرائم اللجوء إلى وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها.

أولا: المقصود بمراقبة الإتصالات الإلكترونية: لم يتطرق الشرع الجزائري شأنه في ذلك شأن أغلب التشريعات المقارنة إلى تحديد ما المقصود بمراقبة الإتصالات الإلكترونية مكتف في ذلك بتحديد مفهوم الإتصالات الإلكترونية فحسب، غير أن الفقه قد تصدى إلى هذه المهمة حيث عرف إجراء المراقبة الإلكترونية على أنه مراقبة شبكة الإتصالات، أو هو العمل الذي يقوم به المراقب بإستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر.

والملاحظ أن التقنية المستخدمة في هذه المراقبة هي التقنية الإلكترونية، والتي تعني مجموعة الأجهزة المتكاملة مع بعضها بغرض تشغيل مجموعة من البيانات الداخلة وفقا لبرنامج موضوع مسبقا للحصول على النتائج المطلوبة،(1)ومن بين تلك التقنيات نجد برنامج كارينفور(2)وتقنية مراقبة البريد الإلكتروني.

ومن الواضح أن الشرع الجزائري لم يعتبر هذا الإجراء من ضمن طرق الحصول على الدليل الرقمي فقط،بل أدرجه ضمن التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية،

فإلى جانب إمكانية القيام بإجراء مراقبة الإتصالات الإلكترونية في إطار التحريات والتحقيقات القضائية من أجل الوصول إلى أدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراءفإنه يمكن كذلك تطويع هذه التقنية لكي تعمل في بيئة الرقابة لغرض الوقاية من إحتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة وهو ما قررته المادة الرابعة من القانون 04/09 بقولها أنه يمكن القيام بعمليات المراقبة الإلكترونية للإتصالات للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة وكذا في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني.

ويعتبر تكريس المشرع لإجراء الراقبة الإلكترونية للإتصالات خطوة جريئة منه على إعتبار أن هذا الإجراء يعد من أخطر الإجراءات في إطار النظام الإجرائي عبر العالم الإفتراضي لكونه يمس مباشرة خصوصيات الإنسان ،وذلك بالرغم من أن البعض من الفقه يرى أن المراقبة لا تزال محل نظر في القانون من حيث ضرورة الإلتزام بما هو مقرر في القوانين والضمانات الدستورية للحق في الخصوصية.

---

(1)مصطفى محمد موسى المراقبة الإلكترونية عبر شبكة الأنترنات دراسة مقارنة بين المراقبة الأمنية التقليدية، دار الكتب والوثائق القومية المصرية الطبعة الأولى 2000، ص205.

(2)قامت إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفدرالي (FBI) بتطوير هذه التقنية وذلك من أجل تعقب وفحص رسائل البريد الإلكتروني المرسلة والواردة عبر أي حاسب خادم تستخدمه أي شركة تقوم بتوفير خدمة الأنترنات ويشتبه في أن تيار الرسائل المار عبر خدماتها يحمل معلومات عن جرائم ويتم تنفيذ عمليات التعقب والفحص بوضع أجهزة الشركة الموفرة للخدمة تحت المراقبة ولقد أصبح يطلق على هذه التقنية بعد أحداث 2011/09/11 تقنية C/CS1000

ثانيا: شروط المراقبة الإلكترونية للإتصالات: أحاط المشرع هذا الإجراء بإعتباره وسيلة إجرائية للحصول على الدليل الرقمي في مجال الجريمة المعلوماتية بمجموعة من الشروط أهمها:

- أن يتم تنفيذ هذا الإجراء تحت سلطة القضاء وبإذن منه، وهو ما كرسته المادة الرابعة من القانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال بنصها على أنه لا يجوز إجراء عمليات المراقبة إلا بإذن من السلطة القضائية المختصة.
- أن تكون هناك ضرورة تتطلب هذا الإجراء وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري أو التحقيق دون اللجوء إلى المراقبة الإلكترونية وهو ما أكد عليه المشرع في الفقرة "ج" من المادة الرابعة في القانون 04/09.

المطلب الثالث:معوقات أو صعوبات التحقيق في الجريمة المعلوماتية:

يتسم التحقيق في الجرائم المعلوماتية بالعديد من المعوقات والصعوبات، فنظرا لوقوع الجريمة المعلوماتية ضمن بيئة رقمية كامنة في أجهزة الحاسب الآلي والخوادم (Serveur) والمضيفات والشبكات بمختلف أنواعها، أدت إلى ظهور نوع من التحدي للأجهزة المختصة بالبحث والتحري في تطبيق القواعد الإجرائية التي نظمت مسألة إستخلاص الدليل الرقمي، وتضعف قيمتها في مكافحة هذا النوع من الجرائم وتؤثر على عملية التحقيق وتؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في أجهزة التحقيق، بل وتنعكس على المجرم نفسه حيث يشعر أن الجهات الأمنية غير قادرة على إكتشاف أمره وأن خبرة القائمين على مكافحة الجريمة والتحقيق فيها لا تجاري خبرته، الأمر الذي يعطيه ثقة أكبر في إرتكاب المزيد من هذه الجرائم.(1)

(1)خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنات، المرجع السابق، ص220.

ولقد كانت هذه التحديات إحدى المسائل الهامة التي ناقشتها المؤتمرات الدولية ولعل أهمها مؤتمر الأنتربول السادس لجرائم تقنية المعلومات الذي شهدته القاهرة في الفترة ما بين 13 إلى 2005./04/15[1]

الفرع الأول:المعوقات المتعلقة بجهات التحقيق وإجراءات الحصول على الدليل:

من أهم المعوقات أو الصعوبات التي قد تواجه التحقيق في الجريمة المعلوماتية معوقات تتعلق بجهات التحقيق وإجراءات الحصول على الدليل، وسوف نحاول أن نتناول ذلك بشيئ من التفاصيل على النحو التالي:

أولا:المعوقات المتعلقة بجهات التحقيق: تتعلق هذه المعوقات بالعامل البشري القائم بالتحقيق في الجريمة المعلوماتية، فإذا كانت السلطات القائمة بالتحقيق من رجال الضبطية القضائية وقضاة بما لها من خلفية قانونية تلعب دورا كبيرا في التحري عن الجرائم والبحث عن مرتكبيها في إطار الجرائم التقليدية فإن وظيفتها في مكافحة الجرائم المعلوماتية لا ترق إلى نفس الدرجة، ذلك أن الطبيعة الخاصة للبيئة الإلكترونية التي تتعامل معها فضلا عن خصوصية الدليل الرقمي ينعكس على عمل الجهات المكلفة بالبحث والتحري.حيث يتطلب الكشف عن هذه الجرائم إكتساب جهات التحقيق مهارات خاصة على نحو يساعدهم على مواجهة التقنيات المعلوماتية،[2]إذ يرى المتخصصون في مكافحة الجرائم المعلوماتية أن الأنظمة المعلوماتية وما يقع عليها من جرائم تعد تحديا هائلا لأجهزة العدالة الجنائية ذلك أن رجل الأمن غير المتخصص والذي إنحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادرا على التعامل مع الجريمة المعلوماتية والتي تقع بطريقة تقنية عالية.

([1])ناقش المؤتمر مجموعة من التحديات ذات أهمية بالغة ولها الأثر في عملية التحري عن الجريمة والمجرم المعلوماتي ومن أهم هذه التحديات:

-التحدي الأول: ويتمثل في إنتشار مقاهي الأنترنات والتي يستطيع أي فرد من خلالها أن يتعامل مع شبكة الأنترنات بما فيه المجرم الذي يستخدمها لإرتكاب جرائمه وهو ما يؤدي إلى صعوبة التوصل إلى مرتكبها نظرا لإمكانية تنقل المجرم بين أكثر من مقهى خلال اليوم الواحد مما يؤدي إلى صعوبة التوصل بصورة دورية لأدلة الإثبات لقيام تلك المقاهي بإعادة تشكيل تلك الأجهزة.

-التحدي الثاني يتمثل في تكنولوجيا الأنترنات فائق السرعة (A.D.S.L)والذي لم يسلم هو الآخر من يد المجرمين إذا إستخدموه لتنفيذ مخططاتهم الإجرامية وذلك عن طريق إشتراكهم إلى جانب أشخاص آخرين في جهاز واحد عن طريق موزع خطوط مما يؤدي إلى صعوبة التوصل إليهم.

-التحدي الثالث: ويتمثل في عمليات التخفي (Proxy) أثناء التجوال عبر الشبكة التي تؤمنها بعض المواقع والتي إستغلت من طرف القراصنة فمصممي الفيروسات المدمرة يقومون بإطلاق فيروساتهم عبر تلك المواقع.

([2])رشيدة بوكر،المرجع السابق ص461.

فنقص المهارة الفنية في إستخدام الكومبيوتر والأنترنات وعدم توفر المعرفة بأساليب إرتكاب الجريمة المعلوماتية وقلة الخبرة في مجال التحقيق والتحري عن جرائم العالم الإفتراضي، عوامل من شأنها أن تضعف دور الأجهزة المختصة بالتحقيق في الجرائم وكشف النقاب عنها، وليس هذا فحسب فإن من المسائل التي تشكل عقبة أمام سلطات التحقيق مسألة كيفية التعامل والحفاظ على الأدلة الرقمية التي مكمنها الحواسيب والخوادم والمضيفات والشبكات.(1)

لأجل ذلك بدأت بعض الأجهزة الأمنية والقضائية في إستقطاب المتخصصين في الكومبيوتر ليكونوا ضمن كوادرها، كما يجري تدريب رجال الضبطية والقضاة على إستخدام الحواسيب وتكنولوجيا المعلومات، وعلى الرغم من ذلك فقد تكون تلك الأجهزة غير قادرة على مواكبة التطور السريع في مجال تكنولوجيا المعلوماتية(2)لعدة أسباب أهمها، أن تكون أمام أجهزة الشرطة والقضاء مجالات متنوعة أخرى ينبغي تغطيتها فهي ليست متفرغة تماما للجرائم المعلوماتية وحدها.

إزاء ذلك يرى البعض أنه من المستحسن أن توكل مهمة التحقيق في هذا النوع من الجرائم إلى جهات متخصصة في هذا المجال سيما مع وجود شركات عالمية متخصصة في تحقيق الجرائم المعلوماتية حققت النجاح في كثير من الحالات.(3)

إلا أن هذا الرأي لم يلق القبول لدى الكثير من الأنظمة القانونية ذلك أن متطلبات العدالة الجنائية تقتضي تحمل الأجهزة الأمنية الحكومية كامل المسؤولية تجاه إكتشاف كافة الجرائم ومن بينها الجرائم المعلوماتية، وفي هذا الصدد ألزمت الإتفاقية الأروبية لجرائم تقنية المعلومات الدول الأطراف بضرورة تبني الإجراءات التشريعية أو أية إجراءات أخرى ترى أنها ضرورية وفقا لقانونها الداخلي من أجل إنشاء وتأسيس سلطات مختصة في مجال التنقيبات والإجراءات الجنائية النوعية في مجال الجريمة المعلوماتية.(4)

---

(1)وضرب المثال على ذلك قيام رجال الشرطة بوضع حقيبة كاملة تحتوي على أسطوانات الكومبيوتر المصادرة في صندوق السيارة بالقرب من جهاز الإرسال والإستقبال اللاسلكي فكانت النتيجة أن الإشارات الكهربائية القوية تسببت في تدميرها جميعا.

(2)محمد أمين البشري التحقيق في الجرائم الحاسب الآلي بحث مقدم لمؤتمر القانون والكومبيوتر والأنترنات كلية الشريعة والقانون بجامعة الإمارات العربية المتحدة 2000/05/03 الطبعة الثالثة 2004، ص107.

(3)مشار إليه لدى خالد ممدوح إبراهيم ،المرجع السابق، ص81.

(4)تم الإشارة إلى هذا الموضوع في المؤتمر الدولي بعنوان الشرطة والأنترنات المنعقد بجامعة السربون باريس في 2005/01/14 وكذا المؤتمر الدولي السادس بشأن الجرائم المعلوماتية المنعقد بالقاهرة في الفترة من 13 إلى 2005/04/15.

وقد بادرت مختلف الدول إلى إنشاء وحدات متخصصة في مجال البحث والتحري عن الجريمة المعلوماتية داخل الأجهزة الحكومية (الضبطية القضائية)[1]ففي فرنسا مثلا قامت بإنشاء عدة وحدات متخصصة وغير متخصصة ضمن جهازي الشرطة والدرك لمكافحة هذا الإجرام المستحدث بجميع صوره ومن ذلك المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والإتصالات[2](OCLTIC) والذي من بين أهم مهامه تقديم المساعدة التقنية لجهات التحقيق وتنسيق الأعمال التحضيرية اللازمة على المستوى الوطني، ويشارك في نشاطات المنظمات الدولية ويحافظ على الروابط العملية بين المصالح المتخصصة في البلدان الأخرى التي تسهر على مكافحة جرائم تقنية المعلومات بصفة عامة والجرائم التي تستهدف نظم المعالجة الآلية لمعطيات بصفة خاصة.بالإضافة إلى قسم الأنترنات التابع للمصلحة التقنية للبحوث القانونية والوثائقية المعروف إختصارا (STRTD)، والقسم الإلكتروني التابع لمعهد البحوث الجزائية التابع للدرك الوطني المعروف إختصارا بـــ (IRCGN) وكذا وحدات أقسام الإستعلامات والتحقيقات القضائية المعرف إختصارا بـــ (BDRIJ). [3]

وفي الجزائرفإنه وبالاضافة الى مصالح الضبطية القضائية التابعة للشرطة أو الدرك فإنه وبموجب المرسوم الرئاسي رقم 183/04 المؤرخ في 2004/06/26 تم إحداث المعهد الوطني للأدلة الجنائية وعلم الاجرام تحت وصاية القيادة العامة للدرك الوطني، حيث تنص المادة الثانية من هذا المرسوم أنه يكلف هذا المعهد بإجراء الخبرات و الفحوص العلمية في إطار التحريات الأولية و التحقيقات القضائية بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات و الجنح، وذلك بناء على طلب من القضاة أو المحققين أو السلطات المؤهلة، ويحتوي هذا المعهد على قسم الإعلام

---

(1)في الولايات المتحدة الأمريكية تم إنشاء داخل مكتب التحقيقات الفدرالي(FBI) إدارة متخصصة لمتابعة جرائم تقنية المعلومات، في إسبانيا أنشأت على مستوى الإدارة المركزية لوزارة الداخلية الإسبانية وحدة التحريات المركزية المعنية بمعلومات جرائم تقنية المعلومات، في مصر أنشأت على مستوى وزارة الداخلية إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، في الأردن تم إنشاء على مستوى مديرية الأمن العام قسم خاص بجرائم تقنية المعلومات يتولى إجراءات التحقيق والإستدلال في هذه الجرائم.

(2)تم إنشاؤه بموجب مرسوم وزاري مشترك رقم (405/2000) مؤرخ في 2000/05/15 على مستوى المديرية المركزية للشرطة القضائية بوزارة الداخلية.

L’ocltic est une structure mixte interministérielle centralisée et opérationelle en matiére de cybercriminalité a compitence nationale et composé de policiers et de gendarmes agissant ensemble dans la lutte contre cybercriminlité. vore plus myriam QUEMENER et joel FERRY cy bercri minalité défi mondial 2 edition 2009p214.

(3)المزيد من التفاصيل حول هذه الأجهزة أنظر:Myriam QUEMENER

الآلي يختص بالتحقيق قي كل ما يتصل بالجرائم المعلوماتية وإلى جانبه يوجدمركز الوقاية من جرائم الإعلام الآلي و الجرائم المعلوماتيةتابع أيضا لقيادة الدرك الوطني وهو قيد الإنشاء، أما على مستوى المديرية العامة للأمن الوطني فتوجد مخابر الشرطة العلمية التابعة لمديرية الشرطة القضائية، ومن الفروع التقنية التي تضمها هذه المخابر، خلية الإعلام الآلي والتي تختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية بناء على تسخيرات أو إنابات قضائية. وحتى تكتمل قدرات تلك الأجهزة في هذا المجال فقد تم إنشاء الهيأة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحته، تتولى هذه الهيأة خصوصا تنشيط وتنسيق عمليات الوقاية من هذا النوع من الجرائم وتعمل على تقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال، بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية كما يوكل لهذه الهيأة عملية تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكان تواجدهم.(1)

وفي إطار محاولة التغلب على المعوقات والصعوبات التي تواجه جهات التحقيق في مجال الجريمة المعلوماتية فإنه من غير الكافي أن يتم إنشاء أجهزة فنية متخصصة، بل لابد من إتباع ذلك بتوفير إستراتيجية تدريبية وتكوين متعمق في ميدان تكنولوجيات الإعلام والإتصال العاملين في مجال العدالة الجزائية بصفة عامة.

ثانيا: المعوقات المتعلقة بإجراءات الحصول على الدليل: إذا كان من السهل على جهات التحري والتحقيق أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة أو التتبع أو سماع الشهود، فإنه قد يصعب عليها ذلك بهذه الطرق بالنسبة للجرائم المعلوماتية التي ترتكب بالوسائل الإلكترونية،(2) وهذا راجع إلى الطبيعة الرقمية التي يتكون منها الدليل التقني سواء من حيث كونه غير مرئي في شكل نبضات مغناطيسية أو كهربائية لا يدركها الرجل العادي بالحواس الطبيعية، أو من حيث تواجده في العالم الإفتراضي على الكيفية المعنوية غير الملموسة ضمن مكون رقمي في شكل مختلط وذلك نتيجة لعدم إمكانية وجود فرز ذاتي في إطار

---

(1) المادتين 13-14 من القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام.و الإتصال

(2) حسين بن سعيد بن سيف الغافري، المرجع السابق، ص413.

التخزين الرقمي، وما يترتب على هذه الخاصية الأخيرة صعوبة في جمع المعلومات الجنائية التي تفيد البحث والتحقيق الجنائي، ذلك لأنها عادة ما تكون مختلطة بغيرها من المعلومات العادية لمستخدمي الحواسيب غير المشتبه فيها وهو أمر قد يشكل تهديدا لخصوصية هؤلاء نظرا لإمكانية إمتداد آثار تفتيش النظام المعلوماتي إليهم.(1)

فضلا عن ذلك فإن المجرم المعلوماتي غالبا ما يضرب سياجا أمنيا على أفعاله غير المشروعة قبل إرتكابه لها، فيزيد بذلك من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه وذلك بالعمل على ترميز أو تشفير المعلومات المخزنة إلكترونيا والمنقولة عبر شبكات الإتصال، بحيث يستحيل على غيره الإطلاع عليها ويصبح بذلك الدليل الرقمي مرمزا أو مشفرا وبالتالي يكون عائقا أمام سلطات البحث والتحقيق أثناء تطبيقها للقواعد الإجرائية المقررة لإستخلاصه.

ومن الصعوبات التي تعيق التحقيق في مجال الجريمة المعلوماتية والمرتبطة بالدليل الرقمي هي سهولة محو هذا الدليل أو تدميره في زمن قصير جدا، فإرتباط الجريمة المعلوماتية بالبيئة التقنية إنعكس على طبيعة الدليل المترتب عنها من حيث أن أمر طمسه ومحو آثاره من قبل الفاعل أمرا في غاية السهولة، إذ بإمكان المستخدم الذي يتحكم في المعلومات أن يستعمل نظاما معلوماتيا من أجل محو تلك المعلومات التي تعد موضوعا للتنقيب الجنائي وبالتالي تدمير كل الأدلة.

فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها بحيث لا تتمكن السلطات من كشف الجريمة، و إذا ما علمت بها لا تستطيع إقامة الدليل ضده(2)

لذلك فإن التحفظ على المعطيات يعتبر إجراء أوليا أو تمهيديا، الهدف منه هو الإحتفاظ بالمعطيات قبل فقدانها.وقد يكون ذلك بالتعاون مع الجهات التي تقدم الخدمة(3)بإلزامهم بطريقة أو بأخرى على حفظ المعطيات المعلوماتية المخزنة بما في ذلك المعطيات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي.(4)

---

(1)خالد ممدوح إبراهيم،المرجع السابق، ص77.

(2)أنظر في ذلك د.غنام محمد غنام، عدم ملاءمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر، دار النهضة العربيةص04 وما بعدها

(3)مقدمو الخدمات حسب التعريف الوارد في المادة 02 الفقرة د من القانون 04/09 هم أي كيان عام أو خاص يقدم لمستعملي خدامته القدرة على الإتصال بواسطة منظومة معلوماتية أو نظام الإتصالات.

(4)لقد حددت المذكر التفسيرية لإتفاقية بوادسيت مبررات إتخاذ هذا الإجراء كما يلي:

وفي هذا الإطار نجد أن المشرع الجزائري قد ألزم في المادة 10 من القانون 04/09 مقدمي الخدمات بحفظ المعطيات المتعلقة بحركة السير و التي حددها في المادة 11 من نفس القانون ووضعها تحت تصرف السلطات المكلفة بالتحريات القضائية.

الفرع الثاني: المعوقات المتعلقة بالجهات المتضررة وصعوبة تحديد الجاني:

بالإضافة إلى المعوقات المتعلقة بجهات التحقيق وإجراءات الحصول على الدليل، فهناك معوقات أخرى تتعلق بالجهات المتضررة والقدرة على تحديد الجاني.

أولا: معوقات التحقيق المتعلقة بالجهات المتضررة: قد يكون للجهات المتضررة من الجريمة المعلوماتية يد في إعاقة التحقيق والوصول إلى الدليل لإثبات الجريمة. فالتقنية المستخدمة في نظم المعلومات تعد مجال إستثمار وتسابق بين الشركات مما يدفعها في مقابل تحقيق الربح إلى تبسيط الإجراءات وتسهيل إستخدام البرامج وملحقاتها وزيادة المنتجات وإقتصار تركيزها على تقديم الخدمة في مقابل إهمال الجانب الأمني، وقد وصل الحد ببعض مستخدمي شبكات الأنترنات عبر مزودي الخدمة في خضم التنافس التجاري إلى درجة عدم مطالبة المشتركين بتحديد هوياتهم عند الإشتراك في خدمة الأنترنات مما يحول دون معرفة هوية المستخدم في حالة البحث والتحري عنها من طرف الجهات للتحقيق، ومن ناحية أخرى فإن كثيرا من الجهات التي تتعرض أنظمتها المعلوماتية للإعتداء تعمد إلى عدم الكشف والتبيلغ عن ذلك لدى السلطات المختصة تجنبا للإضرار بسمعتها أو خوفا من أن الكشف عن أسلوب إرتكاب الجريمة قد يؤدي إلى تكرار وقوعها بتقليدها من طرف الآخرين.

فذاتية الجريمة المعلومية من حيث كونها مجهولة ومستترة تتم في بيئة تقنية لا تترك وراءها أي أثر خارجي تحول دون إكتشافها من طرف المجني عليه، وإذا ما تصادف وإكتشفها فإنه يعمد في أغلب الأحيان إلى التستر عليها والصمت بدل إبلاغ الشرطة للتحقيق بشأنها ومعرفة مرتكبها وهو ما ينجم عنه عدم التعاون مع السلطات المختصة لمكافحة هذا النمط الإجرامي.

1-قابلية المعطيات المعلوماتية للتلاشي حيث تكون محلا للمحو أو التغيير سواء كان ذلك بدافع إجرامي بهدف ضمن معالم الجريمة أو أي عنصر إثباتي لشخص المجرم أو بدافع غير إجرامي في إطار الحذف الروتيني للمعطيات.

2-حفظ المعطيات المعلوماتية التي يمكن أن تتضمن محتوياتها إتصالات غير مشروعة تساعد في تحديد مصدر هذه الإتصالات ومن ثمة تحديد هوية مرتكبي الجريمة.

3-تأمين الدليل التقني من الضياع حيث يتم نسخ دليل على نشاط جنائي من قبل مزودي الخدمة مثل المراسلة الإلكترونية التي تم إرسالها أو إستقبالها ومن ثم يمكن الكشف عن دليل جنائي للجرائم المرتكبة.

لأجل ذلك فقد طرحت العديد من الإقتراحات لحمل المجني عليهم في الجريمة المعلوماتية على التبليغ والتعاون مع السلطات بأن تفرض النصوص القانونية المتعلقة بجرائم المعلوماتية إلتزاما على عاتق موظفي الجهات المجني عليها بالإبلاغ عما يصلهم من أخبار عن وقوع تلك الجرائم مع تقدير الجزاء عن الإخلال بهذا الإلتزام.

ثانيا: صعوبة تحديد هوية الجاني: إن الوصول إلى الدليل الرقمي تعترضه عقبة أخرى تكمن في أن الجناة المتمرسين يجتهدون في إخفاء هوياتهم للحيلولة دون تعقبهم أو كشف أمرهم،[1] بحيث تظل أنشطتهم مجهولة بمنأى عن علم السلطات المعنية بمكافحة الجريمة. ومن الأمثلة التي تساق على ذلك إستخدام الجاني حاسبا آخر غير حاسبه الشخصي كإستخدام الحواسيب الموجودة في الأماكن العامة أو اللجوء إلى مقاهي الأنترنات على إعتبار أن جل هذه المقاهي لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هوياتهم لا سيما إذا علمنا أن شبكة الأنترنات تتيح لمستخدميها إستعمال الخط الواحد من أكثر من شخص في آن واحد معا، ما يجعل المراقبة والتعقب للمشتبه فيه أمرا ينطوي على الصعوبة وغير ميسور في كثير من الأحيان وربما تتعقد المسألة أكثر عند إستخدام الأنترنات اللاسلكي.[2]

وتعد مسألة صعوبة تحديد هوية مرتكب الجريمة المعلوماتية من إحدى المشاكل التي تطرح للكفاح ضد الإجرام المعلوماتي، وإن كان يمكن معرفة النظام أي هوية الحاسوب والخادم والمضيف والشبكات الذي إرتكبت من خلاله.[3]

وقد أشير في المؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلو في الفترة ما بين 29-2000/05/31 موضوع عدم إمكانية البنية التحتية للأنترنات من التوصل إلى تحديد شخصية مرتكب الجريمة أو المصدر الحقيقي لها، وإن كانت توفر إمكانية التعرف على عنوان ورقم الحاسوب فقط المرتبط بالأنترنات والمستعمل كوسيلة لإرتكاب الجريمة عن طريق عنوان IPالذي

([1])موسى مسعود أرحومة، الإشكالات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية بحث مقدم المؤتمر المغاربي الأول حول المعلوماتية والقانون، تنظمة أكاديمية الدراسات العليا طرابلس الفترة من 28-2009/10/29 دون ترقيم

([2])هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء إتفاقية بودايست الطبعة الأولى دار النهضة العربية القاهرة 2006، ص160.

([3])مثل هذا الأمر أوجد إتجاهات في الفقه المقارن تقضي بإعتبار مزود الخدمة للأنترنات مسؤولا عن الجريمة حال عدم معرفة شخصية الجاني الأصلي على أساس مبدأ إفتراض مسؤولية الغير، أنظر في هذا الشأن د عمر أبو بكر يونس الجرائم الناشئة عن إستخدام الأنترنات، مرجع سابق، ص835.

يشير إلى رقم يعين الحاسوب الموصول على الأنترنات. لكن في مقابل ذلك فإن هذا الرقم ليس موحدا على المستوى العالمي، بالإضافة إلى أن مصداقية الهوية عبر الأنترنات(IP) تتقلص كثيرا في بعض الدول إذا علمنا أن كل خط هوية على الأنترنات يصادفه عدد من الهويات التي يمكن أن تكون محلا للتغاير بين أعضاء الأنترنات المشتركين في مزود خدمة واحد، ذلك أن أي شخص يملك هوية رقمية محددة حقا حال وجوده على الأنترنات، إلا أنه إذا حدث وإنقطع الإرسال فإن الشخص نفسه إذا عاد من جديد إلى الأنترنات فإن الهوية السابقة لن تكون له وإنما لغيره ومن الممكن جدا أن يتواجد بهوية (IP) أخرى.

ويزداد الأمر صعوبة حينما تكون المعلومات المحملة في عناوين (IP) غير حقيقية أو زائفة وهذا ممكن حين إستخدام الحزم المعلوماتية (Packet) عنوان IPزائف، بحيث يظهر أن المعلومات جاءت من نظام معالجة محدد بينما في الحقيقة جاء من كومبيوتر آخر ومثال ذلك عندما يقوم برنامج خبيث بإدخال معلومات كاذبة أو غير حقيقية عن عنوان (IP) في حزم الإرسال وقبل الولوج في الشبكة المعلوماتية. لكن يذهب البعض إلى القول أن مسألة عدم معرفة شخصية وهوية الفاعل الذي يتستر وراءها مرسل الرسالة غير المشروعة هو أمر نسبي إذ لا يوجد تجهيل بالمعنى الصحيح بالنسبة لشبكة المعلومات، حيث يترك الفاعل آثارا أثناء تنقله في طرقات شبكات المعلومات تسمح للمحققين من الوصول إليه، والأمر هنا متروك لفطنة رجال الضبطية القضائية من خلال الإستناد إلى فكرة الدلائل الكافية وما ينبثق عنها من شبهات، كما لو كان الحاسوب الذي تم عبره جريمة الإختراق هو حاسوب شخصي وفي هذه الحالة فإن ضبط الحاسوب ذاته يستدعي سؤال صاحبه فيما إذا كان قد إستخدم أحد آخر الحاسوب المذكور أو أن يكون الحاسوب المعني موجودا في الغرفة الشخصية أو كان موجودا في شركة أو مكتب.

وفي كل الأحوال فإن الأمر يتطلب تحسين أسلوب تتبع آثار الرسائل وتحديد هوية المستخدمين حتى يمكن تحديد هوية الشخص المسؤول جنائيا.

وفي هذا الإطار نجد أن المشرع الفرنسي قد أوجب على جميع مزودي خدمات الإتصال للجمهور أن يحددوا على مواقعهم هوية ناشر مضمون الرسالة وبياناته وذلك بموجب المادة 43 من قانون 1986/09/30 وهذا الإجراء من شأنه أن يقدم الكثير من الشفافية بالنسبة للخدمات الموضوعة تحت تصرف الجمهور ويساعد على سهولة تحديد هوية الجاني، بالإضافة كذلك إلى

ضرورة تحديد هوية المشتركين بشبكات المعلومات لتسهيل عمل الضبطية في حال وقوع أي مخالفة بحيث يجب على مؤدي الخدمة أن يكون قادرا على تقديم بيانات شخصية عن زبائنه في إطار التحقيقات عندما يطلب منه ذلك[1]

المطلب الرابع: ضمانات المشتبه فيه أثناء إجراءات الحصول على الدليل الرقمي

إن الخصوصية أو الحق في الحياة الشخصية يعد أحد حقوق الإنسان الأساسية التي أثارت جدلا واسعا على المدى التاريخي، ولعله الحق الذي يعاد التركيز عليه على نحو متعاظم في الوقت الحاضر في ظل التطور التكنولوجي الذي كان له تأثير سلبي على الحياة الخاصة.[2]

ولقد كفلت الدساتير الحماية للحياة الخاصة ومنها الدستور الجزائري،[3]وذلك من خلال منع الغير من الإطلاع عليها بقصد توفير نوع من الإستقرار والأمن للمواطن حتى يتمكن من أداء دوره الإجتماعي. وأن إحداث توازن بين فعالية العدالة الجزائية وضمان الحرية الشخصية هو الذي يعطي الإجراءات الجزائية مصداقيتها في دولة القانون التي تقوم فيها سلطاتها وأجهزتها على إحترام سيادة القانون، لذلك يجب أن تراعي الإجراءات الجزائية حماية الحرية الشخصية في جميع صورها وأشكالها في كافة مراحل الدعوى.

ويتفق فقهاء القانون الجنائي على أن قانون الإجراءات الجزائية يعتبر من القوانين المنظمة للحرية الشخصية للمشتبه فيه وللمتهم، لذلك يعتبر هذا القانون المرآة التي تعكس مدى إحترام حريات وحقوق الأفراد في أي دولة، كما أن قواعد هذا القانون تحاول التوفيق بين مصلحتين متعارضتين هما مصلحة الدولة التي تهدف إلى المصلحة العامة وذلك عن طريق الوصول إلى الكشف عن الحقيقة بغرض إقتضاء الدولة لحقها في العقاب، ومصلحة الفرد بضمان حقوقه وحريته. وأن تغليب إحدى هاتين المصلحتين على الأخرى يحدث خللا في نظام المجتمع إما بقيام نظام إستبدادي بوليسي أو إنتشار الفوضى التي تهدد الأمن والنظام العام.

وهنا تبرز بوضوح مسألة الضمانات في الإجراءات الجزائية وأنها بمثابة الواقي والسياج الحامي للحقوق والحريات، ذلك أنه وإن كان حقا أن الفرد قد أخل بالنظام الأمني الإجتماعي من خلال

---

(1)صالح أحمد البربري، دور الشرطة في مكافحة جرائم الأنترنات في إطار إتفاقية بوادسيت بحث مأخوذ من موقع:
www.arablaw.com

(2)بولين أنطونيوس أيوب،الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة منشورات الحلبي، الطبعة الأولى 2009، ص15.

(3)أنظر المواد:39-40-45-46-47-48 من دستور 1996.

الفعل الجرمي الذي إرتكبه إلا أنه ومع ذلك مازال كما ولد عليه من يقين البراءة، الأمر الذي يوجب التحفظ في معاملته وتقييد المساس بحريتهبالقدر اللازم والضروري لذلك.(1)

وتعد طرق وأساليب جمع الدليل لإثبات الجريمة المعلوماتية من الإجراءات التي من شأنها المساس بالحق في الخصوصية وتعتبر إستثناءا من القاعدة التي تقضي بعدم المساس بحريات الناس وحرمة حياتهم الخاصة، لذلك فقد قيدت التشريعات الإجرائية عند سماحها بذلك سلطات التحري والتحقيق بشروط وشكليات تمثل في حقيقة أمرها ضمانات للمشتبه فيه.

الفرع الأول: ضمانات المشتبه فيه عند إجراء التفتيش وضبط المراسلات الإلكترونية

أسلفنا الحديث بالقول أن الحق في الخصوصية من الحقوق الفردية اللصيقة بشخصية الإنسان وهو من الحقوق الدستورية التي لا يمكن تصور إنسان لا يتمتع بهذا الحق.

وقد إتضح أن إجراء التفتيش يمس بحقوق الأفراد سواء في حريتهم الشخصية أم في حرمة مساكنهم أم مراسلاتهم أم في حياتهم الخاصة، وقد أجيز لضرورة الوصول إلى الحقيقة إجراؤه.لذلك ينبغي أن يقدر بقدره ولا يتعدى نطاق الغرض الذي ابتغي منه.(2)

ولقد أدركت غالبية التشريعات الإجرائية هذه الحقيقة ومنها قانون الإجراءات الجزائية الجزائري، مما حدى به إلى توفير العديد من الضمانات الخاصة بالمشتبه فيه عند تقرير مثل هذا الإجراء، فهل تمتد هذه الضمانات لتشمل حقوق وحريات المشتبه فيه عند تفتيش نظم الحاسوب والأنترنات؟ إن الإجابة على هذا التساؤل تتطلب منا البحث في الضمانات والشروط العامة المقررة عند القيام بإجراء التفتيش ثم مدى أخذ المشرع بها عند ما يعتلق الأمر بتفتيش نظم الحاسوب أو ما يسمى بالتفتيش الإلكتروني La perquisition numirque.

أولا: الضمانات العامة للمشتبه فيه في مواجهة التفتيش وضبط الأدلة:إن التفتيش المعتبر إجراء من إجراءات التحري والبحث عن أدلة الجريمة هو إطلاع المحقق على محل منحه القانون حرمة خاصة لكونه مستودع سر صاحبه وهذا لضبط ما يحتمل وجوده به متى كان ذلك مفيدا للحقيقة، لذلك فكلما وجد السر والكتمان والحماية القانونية وجد التفتيش بشروطه ومتطلباته، أما إذا صرنا إلى العلانية والمجاهرة إنعدم مستودع السر ولا كلام عندئذ عن التفتيش.

(1)محمد محدة، ضمانات المتهم أثناء التحقيق، دار الهدى عين مليلة، الطبعة الأولى 1991-1992، ص6.

(2)محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي دراسة تحليلية نقدية مقارنة للحق في الخصوصية وتطبيقاته في القانون الكويتي، مطبوعات جامعة الكويت 1992، ص156.

وفي حقيقة الأمر فإن تلك الشروط والشكليات والتي قيد بها القانون سلطة التحري والتحقيق عند هذا الإجراء تمثل كلها ضمانات للمشتبه فيه أو للمتهم ومن ذلك:

-لا يصدر الإذن بالتفتيش إلا بعد وقوع جريمة، فحماية للمشتبه فيه من إستخدام هذا الإجراء بصورة غير مشروعة نصت التشريعات الإجرائية ومنها المشرع الجزائري على عدم إمكانية إجراء التفتيش إلا بعد وقوع جريمة، وهو ما يفهم من نص المادة 44 من قانون الإجراءات الجزائية الجزائري ،والسائد في القانون أن إجراء التفتيش لايقع إلا في حالة وقوع جريمة يعتبرها القانون جناية أم جنحة، أما المخالفة فليس في وقوعها ما يبرر مباشرة التفتيش بشأنها لأنها ليست من الأهمية بالقدر الذي يسمح بالتعرض للحرية الشخصية أو إنتهاك حرمة المساكن، كما إستقر الفقه الإجرائي ومعه التشريعات أنه لا يجوز إصدار إذن بالتفتيش بشأن جريمة يحتمل وقوعها مستقبلا.

- تحقيق فائدة مرجوة من إجراء التفتيش ذلك أن الغرض من هذا الإجراء هو إحتمال الحصول على أشياء تفيد في كشف الحقيقة ومن أجل ألا يكون إجراء التفتيش وسيلة للافتئات على حريات الأفراد دون وجه حق فقد قرر الشرع أن يكون هناك فائدة من تقرير هذا الإجراء، وتحقق الفائدة المرجوة من التفتيش تعني أن تقوم قرائن وأمارات على وجود أشياء تتعلق بالجريمة في المكان المراد تفتيشه، وهذا ما يفهم من نص المادة 44 من قانون الإجراءات الجزائية بقولها:" لا يجوز لضباط الشرطة القضائية الإنتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية وأنهم يحوزون أشياء لها علاقة بالجريمة لإجراء التفتيش....." وكذا نص المادة 81 من نفس القانون بقولها أنه يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة.وإذا كان إجراء التفتيش دون فائدة محتملة فإنه يكون تحكميا بسبب إنتفاء المصلحة.[1]

وتقدير ضرورة إجراء التفتيش لتحقيق الفائدة من إجرائه يعود للسلطة القضائية المانحة للإذن به وتتطلب هذه الضمانة أن يقوم القائم بالتفتيش بإجرائه وفقا للكيفية التي تتناسب مع الغرض المرجو من ورائه وهو يختلف بطبيعة الحال حسب نوع الجريمة.

([1])رؤوف عبيد مبادئ الإجراءات الجنائية المصري، مطبعة الإستقلال الكبرى، ط1 القاهرة 1986، ص394.

-لا يتم التفتيش إلا بناءا على إذن مسبق من السلطة القضائية المختصة وهو شرط دستوري[1]نصت عليها المادة 38 من الدستور بقولها أنه لا تفتيش إلا بأمر مكتوب صادر من السلطة القضائية المختصة" وهو ما تؤكده بعد ذلك المادة 44 من قانون الإجراءات الجزائية.

- تحديد ميعاد معين لإجراء التفتيش وهو ما قامت به بعض التشريعات الإجرائية ومنها المشرع الجزائري الذي عمل على تحديد وقت معين لتنفيذ إجراء التفتيش موازنا بين ما يمكن الحصول عليه من أدلة الجريمة وما يمكن حصوله من إضطراب في حياة الناس، واضعا نصب عينيه دائما جسامة الجريمة، فمن كان متهما بجناية ليس كمن هو متهم بجنحة، ومن كان كذلك فإنه لا يجوز تفتيش مسكنه إلا في الأوقات التي حددها المادة 47 من قانون الإجراءات الجزائية وهذا يعني أنه لا يكون قبل الخامسة صباحا ولا بعد الساعة الثامنة مساءا، لكن إذا كان القائم بالتفتيش قد بدأ تفتيشه قبل هذه الساعة و أدركه الوقت و لم ينته تفتيشه فله أن يكمل دون إنقطاع، أما إذا كان الشخص متهما بجناية فإن الشرع أعطى لقاضي التحقيق دون سواه الحق في إجراء التفتيش في غير الساعات المحددة في المادة 47 بشرط أن يجري التفتيش بنفسه دون إنابة قضائية في ذلك وأن يتم بحضور وكيل الجمهورية وهو ما تقول به المادة 82 من قانون الإجراءات الجزائية.

- حضور المشتبه فيه أو المتهم أثناء إجراء التفتيش وهو ما قد إتفقت عليه غالبية التشريعات الإجرائية من ضرورة حضوره أو من ينوب عنه عند عملية التفتيش وهذا حتى يكون على بينة ودراية بما ضبط أو إكتشف، وكضمانة لهذه الحقوق فإن الشرع في حالة رفض المشبه فيه الحضور أو في حالة عدم قدرته على ذلك إشترط حضور من ينوب عنه.

- المحافظة على الأسرار وهي ضمانة نجد لها محلا بنص المادة 45 من قانون الإجراءات الجزائية بنصها:"....غير أنه يجب عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان إحترام ذلك السر" وأعقب الشرع على ذلك بالتجريم والعقاب في المادة 46 لكل شخص يفشي مستندا ناتجا من التفتيش.وفي هذا ضمانة للمشتبه فيه حيث تحفظ أسراره من إطلاع غير المحقق عليها ولو كانوا من مساعديه أو أشخاص آخرين لا صفة لهم قانونا في الإطلاع عليها.

([1])هذا الشرط مطلوب في الدول التي تفصل أنظمتها القانونية بين جهة التحقيق وجهة التحري.

وفيما يتعلق بضبط الأدلة المتحصل عليها بسبب التفتيش فإن الشرع أيضا أحاط هذه العملية بضمانات وشروط منها:

-المحافظة على المضبوطات فقد أوجب المشرع على ضابط الشرطة القضائية الذي وجد أشياء تفيد في مجريات التحريات وأراد ضبطها أن يعرضها على المراد تفتيشه للتعرف عليها وعلى طبيعتها، وفي هذا الإطار نصت المادة 84 من قانون الإجراءات الجزائية أنه:"**....** يجب على الفور إحصاء الأشياء المضبوطة ووضعها في أحراز مختومة ولا يجوز فتح هذه الأحراز إلا بحضور المتهم كما أنه لا يجوز ضبط إلا الأشياء النافعة في إظهار الحقيقة، بل والأكثر من ذلك فقد أجاز المشرع أن يحصل المتهم على صورة فوتوغرافية للأشياء المضبوطة وذلك على نفقته إذا لم يؤثر ذلك على مجريات التحقيق.

ثانيا: ضمانات المشتبه فيه في مجال تفتيش نظم الحاسوبوضبط المعطيات: يتبين من إستقرائنا النصوص القانونية المنظمة لهذا الإجراء أن ما سبق المشرع أن قرره من ضمانات المشتبه فيه حيال إجراء التفتيش قد تتقلص عندما يتعلق الأمر بالبحث والتحري عن الدليل في الجريمة المعلوماتية، وهذا راجع إلى الخصائص التي تتميز بها الجرائم المعلوماتية عن غيرها من الجرائم الأخرى كسرعة تنفيذها ومحو آثارها وبعدها المتخطي للحدود الوطنية ويبدو ذلك من خلال ما يلي:

-إمكانية إجراء التفتيش على المنظومة المعلوماتية بخصوص جرائم معلوماتية يحتمل وقوعها في المستقبل وهذا خلافا لما سبق وأن مر بنا من أنه لا يصدر الإذن بالتفتيش إلا بعد وقوع جريمة ويفهم ذلك من نص المادة 05 من القانون 04/09 التي أجازت للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول إلى المنظومة المعلوماتية أو جزء منها بغرض القيام بتفتيشها من أجل الوقاية من أفعال إرهابية أو تخريبية أو الوقاية من جرائم ماسة بأمن الدولة، بالإضافة إلى إمكانية القيام بهذا الإجراء في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية يكون غرضها تهديد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.

فإستعمال الشرع لمصطلحي "من أجل الوقاية"، و"إحتمال إعتداء" يفهم منهما أن القانون 04/09 قد أجاز اللجوء إلى إجراء التفتيش في الجرائم المعلوماتية حتى ولو لم تقع جريمة

بعد.لكنونظرا لخطورة هذا الإجراء على الحق في الخصوصية فإن الشرع قد حصر نطاقه في حالات محددة على سبيل الحصر[1]

-وقد تمسك المشرع بشرط ضرورة أن تكون هناك فائدة مرجوة من إجراء التفتيش والذي يعني كما سبق الذكر قيام قرائن وأمارات على وجود أشياء تتعلق بالجريمة في المحل المراد تفتيشه وذلك حينما إشترطت المادة 02/05 من القانون 04/09 الدخول إلى المنظومة المعلوماتية بغرض تفتيشها بضرورة أن تكون هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة فعلا في هذه المنظومة محل التفتيش، كما يفهم من نص المادة 06 من القانون04/09 أنه إذا كان ليس من الضروري حجز كل المنظومة المعلوماتية فإن السلطة التي تباشر التفتيش تقوم فقط بنسخ المعطيات التي تكون مفيدة في الكشف عن الجرائم أو مرتكبيها و هذا ما يعد ضمانة أخرى.

- أما عن شرط تحديد ميعاد معين لإجراء التفتيش فإن الشرع قد تنازل صراحة عن هذا الشرط في الجرائم المعلوماتية وأجاز القيام بإجراء التفتيش على المنظومة المعلوماتية وكذا الأماكن التي يتواجد بها الحاسوب في أي ساعة من ساعات الليل والنهار،[2]وربما يعد ذلك إنسجاما مع خصائص الجريمة المعلوماتية. ذلك أن الطابع الدولي لهذه الجريمة يعني إرتكابها من عدة دول في نفس الوقت وهذا يعني أن الوقت في بعضها قد يكون ليلا بينما في دول أخرى يكون نهارا إضافة إلى طابع السرعة الذي يميز إرتكاب الجريمة المعلوماتية وكذا محو آثارها.

- كما نجد أن الشرع الجزائري أصبح لا يشترط حضور المشتبه فيه أو من ينوبه عملية التفتيش في الجريمة المعلوماتية وهو ما نص عليه صراحة في المادة 6/45 بقولها أنه لا تطبيق الأحكام المنصوص عليها في هذه المادة إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

- أما المحافظة على الأسرار وهي الضمانة التي تقررها المادتين 08-09 من القانون 04/09 إذ قرر المشرع من خلالهما أنه يمكن للسلطة التي تباشر التفتيش أن تأمر بإتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، وأنه لا يجوز إستعمال المعلومات المتحصل عليها إلا في الحدود الضرورية للتحريات والتحقيقات القضائية وهذا تحت طائلة العقوبات المنصوص عليها في التشريع المعموله به.[3]فإذا كان المشرع قد خول لجهات التحقيق المختصة حق الإطلاع

([1])أنظر المادة 03 من القانون 04/09.

([2])المادة 3/47 من قانون الإجراءات الجزائية.

([3])أنظر المادة 46 من قانون الإجراءات الجزائية.

على بعض الأسرار المفيدة في كشف الحقيقة فإن عليها ألا تتوسع في ذلك، فإذا كان ضابط الشرطة القضائية يبحث عن برنامج على ذاكرة الحاسوب الرئيسية فيجب عليه ألا يقوم بفتح الملفات الخاصة بأسرار المشتبه فيه والإطلاع عليها[1]إلا إذا كانت هذه الملفات تتعلق بالجريمة المعلوماتية المرتكبة.وفيما يتعلق بضبط المعطيات المعلوماتية المتحصل عليها بسبب تفتيش منظومة معلوماتية فقد أحاطها المشرع هذه العملية أيضا بضمانات وشروط أهمها:

- المحافظة هلى المضبوطات وذلك بالطريقة التقنية التي تتناسب معها حيث أوجب المشرع في المادة 01/06 من القانون 04/09 أن يتم ضبط المعطيات المخزنة في المنظومة بنسخها على دعامة تخزين إلكترونية تكون قابلة للوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

كما أوجب الشرع أيضا على السلطة التي تقوم بضبط المعطيات العمل على سلامة المعطيات في المنظومة المعلوماتية محل التفتيش وأنه إذا ما استعملت تقنيات لإعادة تشكيل هذه المعطيات قصد جعلها قابلة للإستغلال فإن ذلك يجب ألا يؤدي إلى المساس بمحتواها.

الفرع الثاني :ضمانات المشتبه فيه أثناء إجراء إعتراض المراسلات والمراقبة الإلكترونية:

مما لاشك فيه أن مراقبة الإتصالات الخاصة[2]وكذا إعتراض المراسلات يمس[3] بحق الإنسان في الخصوصية ويعد إعتداء صارخا على الحياة الخاصة، ذلك الحق الذي حظي بحماية دستورية في مختلف التشريعات الحديثة، لما لخصوصية الأفراد من أهمية قصوى على كيان الفرد والمجتمع معا والحق في الخصوصية وما يتفرغ عنه من حرية المراسلات وسرية الأحاديث الخاصة أضحى في الوقت الراهن تحت تهديد وسائل تقنية حديثة إخترقت الحجب ونفذت من خلال السياج المنيع الذي يحيط بالحياة الخاصة.

ولقد كفلت القوانين للفرد حقه في خصوصية مراسلاته بغض النظر عن وسيلة إرسالها سواء كانت مرسلة بواسطة البريد العادي أم بواسطة الأنترنات (البريد الإلكتروني (Email) وسواء كانت هذه الرسالة مغلقة أم مفتوحة مشفرة أم غير مشفرة، طالما أن من الواضح قصد المرسِل عدم رغبته في إطلاع الغير عليها بدون تمييز، وبالتالي فإن حرمة المراسلات مستمدة من الحق في الحياة الخاصة لأنها تعتبر مستودعا للسر فلا يجوز المساس بها إلا بموافقة من يتعلق الخطاب بحياته الخاصة.

(1)صبري عبد المجيد و صبري حمد خاطر، الحماية القانونية للملكية الفكرية، بيت الحكمة بغداد، الطبعة الأولى 2001، ص264.

(2)المادة 03 من القانون 04/09.

(3)المادة 65 مكرر 05 من قانون الإجراءات الجزائية.

وإسترشادًا على ذلك نصت المادة الثامنة في فقرتها الأولى من الإتفاقية الأروبية لحقوق الإنسان على أن لكل شخص الحق في إحترام حياته الخاصة والعائلية وموطنه ومراسلاته، وحظرت في الفقرة الثامنة على السلطات الحكومية أي تدخل أو إعتراض المراسلات أو الإتصالات الإلكترونية إلا إذا نص القانون على ذلك، وأن يكون لضرورة تتعلق بالنظام أو الأمن القومي أو إقتصاد الدولة أو المنع والوقاية من الجرائم أو لحماية الصحة العامة والأخلاق ولحماية حقوق و حريات الغير.

كما قد حظي مبدأ خصوصية المراسلات في فرنسا بتشريع خاص به وهو القانون المتعلق بالإتصالات عن بعد[1]الصادر في 1991/07/10، والذي نص صراحة على أن سرية المراسلات التي تتم عن بعد يكفلها القانون ولا يجوز المساس بسريتها إلا بواسطة السلطة العامة(النيابة العامة) وفي حالات المصلحة العامة وبالشروط المنصوص عليها والمحددة قانونا.[2]

والوضع ذاته في التشريع الأمريكي فبالإضافة إلى التعديل الرابع للدستور الأمريكي الذي عزز مفهوم الخصوصية، صدر قانون خصوصية الإتصالات الإلكترونية عام 1986الذي نص في الباب الأول منه على حظر كل إعتراض غير مرخص به للإتصالات التي تأخذ الطريق الإلكتروني وحظر كذلك الدخول غير المسموح به للرسائل والبيانات الموجودة على ذاكرة الحاسوب واشترط لمشروعية ذلك ضرورة الحصول على إذن من القضاء[3]

و لم يكن الشرع الجزائري في غيبة عن هذا الأمر، إذ أنه وبموجب القانون 23/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون العقوبات أضاف المادة 303 مكرر التي تعاقب بالحبس لكل من يتعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت وذلك بإلتقاط أو تسجيل أو نقل مكالمات أو أحاديث أو سرية، بالإضافة إلى المادة 127 من القانون 2000/03 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية التي تنص كذلك على معاقبة كل شخص سواء كان مرخصا له بتقديم خدمة المواصلات السلكية واللاسلكية أو كان عاملا لدى متعاملي

([1])يقصد بالإتصال عن بعد كل إنتقال أو إرسال أو إستقبال لرموز أو إشارات أو كتابة أو أصوات أو معلومات أيا كانت طبيعتها بواسطة ألياف بصرية أو طاقة لا سلكية أو أي أنظمة إلكترومغناطيسية أخرى.

([2])وفي قانون العقوبات الفرنسي نصت الفقرة الثانية من المادة 432 على معاقبة كل شخص عام أو مكلف بخدمة عامة إذا قام أو أمر أو سهل أثناء مباشرته لعمله أو بمناسبته وفي غير الحالات المقررة قانونا بإلتقاط أو إختلاس مراسلات تتم أو تنقل أو تحمل بطريق الإتصالات وكذا إستعمالها أو فض محتواها.

([3]) نشوى رأفت إبراهيم،المرجع السابق، ص13.

الشبكات العمومية للمواصلات السلكية واللاسلكية أو أي شخص آخر غير هؤلاء يقوم بأي طريقة كانت بإنتهاك سرية المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق المواصلات السلكية أو اللاسلكية.

إلا أن هذه الحماية الجزائية لسرية المراسلات والإتصالات ليست مطلقة على حالها، ذلك أنه إذا تعلق الأمر بمسألة تهديد أمن الدولة ومواطنيها أو إحتمال حدوث أفعال من شأنها المساس بالنظام العام، فإن المشرع قدر أن هذه المسائل تعلو على حق المشتبه فيهم في خصوصية مراسلاتهم وإتصالاتهم، لأجل هذا أجاز إعتراض هذه المراسلات ومراقبة الإتصالات إما كإجراء تحقيقي أو كإجراء وقائي.

وإذا كان المشرع قد أباح وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميعمحتواها وكذا إعتراض المراسلات السلكية واللاسلكية، فإنه قد أحاط هذه الإجراءات بمجموعة من الضمانات التي تعد ضرورية لحماية حق الإنسان في سرية إتصالاته. وهذا ما يمكن أن نجمله في ما يلي:

أولا: ضمـــانات المشتبه فيه عند إعتـــراض المـــراسلات: لم يجز المشرع للضبطية القضائية إجراء إعتراض الراسلات السلكية أو اللاسلكية إلا بموجب إذن مكتوب من السلطة المختصة والمتمثلة في وكيل الجمهورية في حالة التحقيق الإبتدائي، أو قاضي التحقيق في حالة ما إذا فتح تحقيق قضائي.[1]وهو ما يجعل هذه العمليات تكون في ضمانة من أهم الضمانات الإجرائية وهي سلطة القضاء.

كما إشترط المشرع ضرورة أن يتضمن الإذن الممنوح من الجهة القضائية المختصة وصفا للمراسلات التي يجب إعتراضها، وذلك ببيان العناصر التي تسمح بالتعرف على هذه المراسلات المطلوبة بالإضافة إلى تحديد المدة التي تستغرقها التدابير التقنية اللازمة في عملية الإعتراض،[2]وهنا حدد الشرع مدة الإذن بأربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.

([1])المادة 65 مكرر 5 من قانون الإجراءات الجزائية:".... يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي: إعتراض المراسلات التي تتم عن طريق الإتصالات السلكية أو اللاسلكية وفي حالة فتح تحقيق قضائي تتم العمليات المذكورة بناءا على إذن من قاضي التحقيق. ونصت المادة 04 من القانون 09/04".... لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية المختصة".

([2])أنظر المادة 65 مكرر 07 من قانون الإجراءات الجزائية.

ومن بين الضمانات التي تحيط بهذه العملية أيضا هو وجوب تحديد ساعات الإعتراض وذكر ذلك في المحضر الذي يحرره ضابط الشرطة القضائية عن كل عملية إعتراض يقوم بها، وهو ما نصت عليه المادة 65 مكرر" يحرر ضابط الشرطة القضائية.... محضرا عن كل عملية إعتراض للمراسلات ويذكر بالمحضر تاريخ وساعة بداية هذه العمليات والإنتهاء منها.

بالإضافة إلى ذلك فقد ألزم المشرع بنص المادة 65 مكرر 10 من قانون الإجراءات الجزائية ضابط الشرطة القضائية أن ينسخ فقط المراسلات والمحادثات التي تكون مفيدة في إظهار الحقيقة.

ثانيا: ضمانات المشتبه فيه أثناء مراقبة الإتصالات:في الحقيقة أن هذا الإجراء محاط بكثير من القلق الذي يبديه رجال القانون دفاعا عن الحريات الخاصة، إلا أن المسألة في النهاية تتوقف على قدرة المشرع في إقامة التوازن بين حق المجتمع في الأمن ومنع الجريمة وحق الأفراد في السرية، وذلك بإجازة اللجوء إلى هذا الإجراء لكن مع ضمان عدم التعسف في إستخدامه من خلال إحاطته بجملة من الشروط.

وقد استهل المشرع نص المادة الثالثة من القانون 04/09 بإشتراط القيام بإجراء المراقبة الإلكترونية للإتصالات في إطار إحترام الأحكام القانونية التي تضمن سرية المراسلات والإتصالات حينما نصت:" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات..... يمكن وضع ترتيبات لمراقبة الإتصالات.....".

كما حدد المشرع في نص المادة 04 من نفس القانون صراحة الحالات التي يجوز فيها اللجوء إلى هذا الإجراء إذا كان الغرض منه الوقاية فقط دون أن تكون هناك جريمة قد وقعت أصلا وذلك كوسيلة لإجهاض المشروعات الإجرامية التي يكون الهدف منها النيل من المصالح الكبرى للدولة ويكون من الصعب معالجة آثارها إذا تحققت فعلا، مقدرا خطورة وجسامة هذه الأفعال والتي منها الأفعال الموصوفة بالجرائم الإرهابية والجرائم المساة بأمن الدولة أو الإعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.أما في إطار التحريات و التحقيقات القضائية فإنه لا يتم اللجوء الى اجراء المراقبة الالكترونية للاتصالات الا في الحالة التي يكون فيها من الصعب الوصول الى نتيجة تهم هذه التحقيقات دون اللجوء الى هذا الاجراء.

وإن كان المشرع قد ألزم في كل إجراء من شأنه المساس بالحريات عدم جواز القيام به إلا بموجب إذن من السلطة القضائية المختصة،فإنه إشترط في المادة الرابعة الفقرة السادسة من القانون09/04 أنه لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية. إلا أننا نرى أنه كان على المشرع تحديد مدة المراقبة كما فعل بشأن اعتراض المراسلات، لأن المراقبة الإلكترونية المفتوحة تتعارض مع الغاية منها والتي يجب أن تكون في أضيق حدودها ذلك أن إطالة وقت المراقبة فيه إطلاع وكشف لأسرار الأشخاص دونما مبرر.(1)

(1)تكلم المشرع عن تحديد مدة المراقبة في حالة واحدة فقط تتعلق بالمراقبة الإلكترونية التي يقوم بها ضباط الشرطة القضائية المنتمين إلى الهيأة الوطنية للوقاية من الجرائم المتحصلة بتكنولوجيات الإعلام والإتصال بخصوص تحريهم للوقاية من أفعال موصوفة بجرائم الإرهاب والجرائم الماسة بأمن الدولة وهي ستة أشهر قابلة للتجديد.

المبحث الثالث:

القيمة القانـــونية للدليل الرقمي في مجال الإثبات الجنائي:

لقد توجس كل من الفقه والقضاء خيفة من الدليل الرقمي لإمكانية عدم تعبيره عن الحقيقة نظرا لما يمكن أن تخضع له طرق الحصول عليه من التعرض والتزييف والتحريف والعبث، وهو ما يثير مسألة مشروعية الأخذ به، إذ يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا من حيث وجوده ومن حيث الحصول عليه.

كما يثير أيضا مسألة مصداقية أو حجية الدليل الرقمي في تعبيره عن الحقيقة التي تهدف إليها الدعوى الجزائية لاسيما إذا أخذنا بالإعتبار الصعوبات التي تصاحب إستخلاصه، فضلا عن التطور في مجال المعلوماتية الذي قد يتيح العبث بهذا النوع من الأدلة بما يجعل مضمونها مخالفا للحقيقة وعلى ذلك فكيف نضمن مصداقية هذه الأدلة وتكون لها الحجية في الإثبات، وما مدى إقترابها نحو الحقيقة؟ وهل مفهوم الحجية التي يجب أن يتمتع بها الدليل الجنائي يتعارضمع الطبيعة الخاصة للدليل الرقمي.

إن مجرد وجود دليل يثبت وقوع الجريمة ونسبتها إلى شخص معين لا يكف للتعويل عليه، إذ يلزم أن تكون لهذه الأدلة قيمة قانونية، وقيمة الدليل الجنائي تتوقف على مسألتين رئيسيتين: الأولى هي مشروعية الدليل والثانية هي حجية الدليل على الوقائع المراد إثباتها.

المطلب الأول: مشروعية الدليل الرقـــــمي

تعرف المشروعية بأنها التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام، فهي تهدف إلى تقرير ضمانة أساسية وجدية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة ومن التطاول عليها في غير الحالات التي رخص فيها القانون بذلك، من أجل حماية النظام الإجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته.[1]

لذلك فإنه لصحة الإجراءات التي تقوم بها جهة التحقيق أن تغلف بمبدأ المشروعية من أجل أن تثمر على دليل صحيح وسليم يعول عليه القضاء في أحكامه.

فلا شك أن مبدأ شرعية الجرائم والعقوبات الذي يستقيم عليه بنيان القانون الجنائي الموضوعي ينعكس على قواعد الإثبات الجنائي ويفرض خضوعها هي الأخرى لمبدأ الشرعية، والتي

---

(1)هلالي عبد الله أحمد، حجية المخرجات الكومبيوترية في المواد الجنائية،الطبعة الثانية دار النهضة العربية 2008، ص104.

تستلزم عدم قبول أي دليل يكون البحث عنه أو الحصول عليه قد تم بطريقة غير مشروعة، وتعد مسألة قبول الدليل الجنائي بصفة عامة الخطوة الأولى التي يتخذها القاضي الجزائي تجاهه وذلك بعد التنقيب عنه وقبل إخضاعه لتقديره، وقبول الدليل على هذا النحو يتسع ويضيق تبعاً للمبادئ التي تقوم عليها أنظمة الإثبات السائدة.

والحقيقة أن مشروعية الدليل الرقمي هي مشروعية وجود ومشروعية حصول.

الفرع الأول: مشروعية وجود الدليل الرقـــمي:

تقتضي مشروعية وجود الدليل الرقمي أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الإثبات الجنائي

أولا: المقصود بمشروعية الوجود:ويقصد بمشروعية وجود الدليل الرقمي أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها للقاضي الإستناد إليه في تكوين عقيدته، ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الرقمي يتمثل في طبيعة نظام الإثبات السائد في الدولة، إذ تختلف النظم القانونية في موقفها من حيث الأدلة التي يمكن قبولها في الإثبات.

ثانيا: موقف المشرع الجزائري من الدليل الرقمي: لقد عرفت التشريعات الإجرائية الجزائية نظامين رئيسين للإثبات هما:

- نظام الإثبات المقيد وفيه يقوم المشرع بتحديد أدلة الإثبات حصرا وكذا القوة الإثباتية لكل دليل من الأدلة بناءا على قناعة المشرع بها.وهو ما يعرف بنظام الأدلة القانونية، إذ لا يكون لقناعة القاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، فتحدد للقاضي الأدلة التي يجوز له قبولها واللجوء إليها في الإثبات ولا سبيل للإستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات.

- نظام الإثبات الحر والذي يقوم على أساس حرية الإثبات فلا يقوم المشرع بتحديد الأدلة بل يكون للقاضي دور إيجابي في البحث عن الأدلة وتقدير قوتها الثبوتية حسب قناعته بها، فلا يلزمه القانون بأدلة للإستناد إليها في تكوين قناعته فله أن يبني هذه القناعة على أي دليل وإن لم يكن منصوصا عليه، بل إن المشرع في مثل هذا النظام لا يحفل بالنص على أدلة الإثبات فكل الأدلة تتساوى قيمتها الإثباتية في نظر المشرع، والقاضي هو الذي يختار من بين ما يطرح عليه ما يراه

صالحا للوصول إلى الحقيقة وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يطمئن إليه، فلا يتدخل المشرع في تحديد القيمة الإقناعية للدليل ولذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في مجال الإثبات في مقابل إنحصار دور المشرع.[1]

وعلى هذا الأساس وإسترشادا بما سبق ذكره فإن النظم القانونية التي تتبنى نظام الأدلة القانونية لا يمكن في ظلها الإعتراف للدليل الرقمي بأية قيمة إثباتية ما لم ينص القانون عليه صراحة ضمن قائمة أدلة الإثبات، ومن ثم فإن خلو القانون من النص عليه سيهدر قيمته الإثباتية مهما توافرت فيه شروط اليقين، فلا يجوز للقاضي أن يستند إليه لتكوين قناعته.[2]وتطبيقا لهذا الفهم نص قانون الإثبات في المواد الجنائية البريطاني على قبول الدليل الرقمي وحدد قيمته الإثباتية تجاوبا وإتفاقا مع طبيعة النظام القانوني في بريطانيا.[3]

ويمكن أن يعاب على نظام الإثبات القانوني أن من شأنه تقييد القاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته للنصوص القانونية لذلك فإن هذا النظام بدأ ينحصر نطاقه حتى في الدول التي تعتبر الأكثر إعتناقا له.

ففي بريطانيا مثلا بدأت تخفف من غلوائه حيث ظهر فيها ما يعرف بقاعدة الإدانة دون أدنى شك والتي مفادها أن القاضي يستطيع أن يكون قناعته من أي دليل وإن لم يكن ضمن الأدلة المنصوص عليها متى كان هذا الدليل قاطعا في دلالته.

أما بالنسبة للنظم القانونية التي تعتمد نظام الإثبات الحر كما هو الحال عليه في القانون الجزائري[4](المادة 212 من قانون الإجراءات الجزائية) والقانون الفرنسي (المادة 427 قانون الإجراءات الجزائية الفرنسي) فإنه لا تثور مشكلة مشروعية الدليل الرقمي من حيث الوجود، على إعتبار أن المشرع لا يعتمد سياسة النص على قائمة لأدلة الإثبات فالأساس هو حرية الأدلة، لذلك

(1)هلالي عبد اللاه أحمد، حجية المخرجات الكومبيوترية، المرجع السابق. ص29،

(2)طارق محمد الجملي الدليل الرقمي في مجال الإثبات الجنائي، المرجع السابق، ص23.

(3)الدول ذات الثقافة الأنجلوسكونية مثل بريطانيا والولايات المتحدة الأمريكية أخذت بنظام الإثبات القانوني.

(4)هناك العديد من الأسباب التي تبرر الأخذ بمبدأ حرية الإثبات في نطاق نظرية الإثبات الجزائي منها أن حرية الإثبات تعد نتيجة منطقية لمبدأ أن القاضي يقضي بمحض إقتناعه الذاتي والتي تستلزم بالضرورة منح الحرية للقاضي بالإستعانة بجميع وسائل الإثبات التي يقتنع ويطمئن إليها حتى يتسنى له أداء رسالته في إرساء العدالة بين المتقاضين، بالإضافة إلى أن الإثبات في الدعوى الجزائية يرد على وقائع مادية يصعب بل قد يستحيل الحصول على دليل مسبق لها وذلك بعكس الدعوى المدنية التي يرد الإثبات فيها على تصرفات قانونية يسهل إعداد دليل مسبق بشأنها.

فمسألة قبول الدليل الرقمي لا ينال منها سوى مدى إقتناع القاضي به إذا كان هذا النوع من الأدلة يمكن إخضاعه لتقدير القاضي وهو ما سوف نتناوله لاحقا عند الحديث على حجية الدليل الرقمي.

وفي هذا الصدد فإن المشرع الجزائري وكغيره من التشريعات المنتمية إلى نظام الإثبات الحر لا نجده قد أفرد نصوصا خاصة تحظر على القاضي مقدما قبول أو عدم قبول أي دليل بما في ذلك الدليل الرقمي، وهو أمر منطقي طالما أن المشرع الجزائري يستند لمبدأ حرية الإثبات حيث لم يتضمن قانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها أية أوضاع خاصة وترك الأمر للقواعد العامة، ومنها أن الأصل في الأدلة مشروعية وجودها ومن ثم فإن الدليل الرقمي سيكون مشروعا من حيث الوجود إصطحابا للأصل، ومن جهة أخرى فإنه وطبقا لمبدأ الشرعية الإجرائيةفلا يكون الدليل مقبولا في عملية الإثبات إلا إذا كان مشروعا ذلك أن القاضي لا يقدر إلا الدليل المقبول ولا يكون كذلك إلا إذا كان مشروعا بأن تم البحث عنه والحصول عليه وفقا لطرق مشروعة.

الفرع الثاني: مشروعية الحصول على الدليل الرقمي:

إنه من الضروري أن يتم رسم ضوابط وأطر معينة يتعين أن تمارس في نطاقها عملية البحث عن الأدلة وتحصيلها والتحقيق فيها، بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع من ورائها وهو الوصول إلى الحقيقة الفعلية في الدعوى وهي الهدف الأسمى لقانون الإجراءات الجزائية.

أولا: المقصود بمشروعية الحصول على الدليل الرقمي:إنه من المقرر أن الإدانة في أي جريمةلابد وأن تكون مبنية على أدلة مشروعة تم الحصول عليها وفق قواعد الأخلاق والنزاهة وإحترام القانون من طرف الجهة المختصة بجمع الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية، و لا يكون مشروعا إلا إذا أجرى التنقيب عنه أو الحصول عليه أوكانت عملية تقديمه إلى القضاء أو إقامته أمامه بالطرق التي رسمها القانون، فمتى ما تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد بقيمته مهما كانت دلالته الحقيقية وذلك لعدم مشروعيته، وعلى هذا الأساس فإن إجراءات جمع الأدلة الرقمية المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة، وبالتالي بطلان الدليل المستمد منها ولا تصلح لأن تكون أدلة تبنى عليها الأدانة في المواد الجنائية. وفي إطار مشروعية الأدلة

الرقمية نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة والنزاهة في البحث عن الحقيقة إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية أم في مجال التنقيب في الجرائم المعلوماتية، ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل إستخدام الوسائل العلمية الحديثة في عملية البحث والتحري عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية ومن بينها الأدلة الرقمية بطريقة شرعية ونزيهة.(1)وقد قضي في هلندا أنه إذا كانت بيانات الحاسوب المسجلة في ملفات الشرطة غير قانونية فذلك يؤدي إلى نتيجة مؤداها ضرورة محو هذه البيانات وعدم إمكانية إستخدامها كدليل جنائي بسبب مبدأ إستبعاد الأدلة غير القانونية.ومن قبيل الادلة غير المشروعة الحصول غلى على دليل رقمي من خلال اجراء مراقبة الاتصالات دون ان يكون محلا لاذن من السلطة القضائية المختصة او اتخاذ ترتيبات تقنية من أجل تفتيش منظومة معلوماتية تؤدي إلى المساس بالحياة الخاصة للغير أو ممارسة الإكراه المادي أو المعنوي في مواجهة المشتبه فيه من أجل فك شفرة نظام من النظم المعلوماتية أو التحريض على إرتكاب الجريمة عن طرف الضبطية،(2)ويعد من الطرق غيرالمشروعة أيضا إستخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الإلكترونية.

ولقد صادقت لجنة الوزراء التابعة للمجلس الأروبي في 1981/01/28 على إتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الإتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة ومستمدة بطرق مشروعة وعدم إفشائها أو إستعمالها في غير الأغراض المخصصة لها،كما أن للشخص المعني الحق في التعرف والإطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة(3)

ولقد وضعت الدساتير والقوانين الإجرائية نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية، ومن ثم مخالفة هذه النصوص في إستخلاص الدليل يصبغ هذا الدليل بالامشروعية والقول بذلك يهدر قيمته، فمشروعية الدليل تتطلب صدقه في مضمونه وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة تدل على الأمانة والنزاهة من حيث طرق الحصول عليه.

(1)علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنات عالم الكتب الحديثة الأردن، ص186.

(2)علي حسن محمد الطوالبة، المرجع السابق، ص189.

(3)مشار إليه لدى رشيدة بوكر، المرجع السابق. ص492،

والحقيقة أن مشروعية الدليل تعد قيدا وخطا فاصلا بين حق الدولة في توقيع العقاب لضمان أمن وإستقرار المجتمع من جهة، وبين ضمان حقوق الأفراد وحرياتهم من جهة أخرى لذلك فالسؤال المطروح في هذا الإطار ما هو موقف القضاء من الدليل غير المشروع وما هي قيمته في الإثبات الجنائي؟

ثانيا: موقف القضاء من الدليل غير المشروع: إن هذا التساؤل يقود إلى بحث قيمة كل من دليل الإدانة ودليل البراءة لمعرفة قيمته في الحالتين:

فالبنسبة لدليل الإدانة فإن الأمر يقتضي من أجل كسر قرينة البراءة التي يتمتع بها المتهم أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة،[1] ويستوي في ذلك إن كانت أدلة تقليدية أم مستخلصة من الوسائل الإلكترونية. وأي دليل تم الحصول عليه بطريقة غير مشروعة أو بوسيلة مخالفة للقانون يعتبر غير مقبول في عملية الإثبات لأنه إذا ما سمح بقبول أدلة وليدة عن إجراءات باطلة أدى ذلك إلى إهدار الضمانات التي كفلها القانون لحماية حقوق المواطن وكرامته، وترتيبا على ذلك فإنه لا يجوز للقاضي القبول بدليل رقمي تم الحصول عليه من إجراء التسرب جرى القيام به دون مراعاة الشروط الشكلية والموضوعية للإذن بمباشرة هذا الإجراء، أو كان الدليل متحصلا عليه عن طريق إكراه المتهم المعلوماتي من أجل فك شفرة للدخول إلى النظم المعلوماتية أو كلمة السر اللازمة للدخول إلى ملفات المعلومات المختزنة أو القيام بإجراء التنصت أو المراقبة الإلكترونية عن بعد دون مسوغ قانوني، ويكون الدليل المتحصل عليه وفق الطرق السابقة باطلا وعدم إنتاج الآثار القانونية المترتبة عليه.

والقاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة له مباشرة وهو الرأي الراجح الذي أخذ به الشرع الجزائري بنص المادة 191 من قانون الإجراءات الجزائية التي نصت على أنه تنظر غرفة الإتهام في صحة الإجراءات المرفوعة إليها وإذا تكتشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الإقتضاء ببطلان الإجراءات التالية له كلها أو بعضها. وقد أوصى المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوباتفي مجال حركة إصلاح الإجراءات الجنائية وحماية حقوق الإنسان بمجموعة من التوصيات منها التوصية رقم 18 التي تنص على أن كل الأدلة التي تم الحصول عليها عن طريق إنتهاك حق أساسي للمتهم والأدلة الناتجة عنها

[1] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي،و التكنولوجيا الحديثة،دار النهضة العربيةالقاهرة2002 ،ص111.

تكون باطلة ولا يمكن التمسك بها أو مراعاتها في أي مرحلة من مراحل الإجراءات، وقد أشار هذا المؤتمر إلى ضرورة إحترام مبدأ المشروعية عند البحث عن الدليل في الجرائم المعلوماتية في بيئة تكنولوجيا المعلومات وإلا ترتب عليه بطلان الإجراء.

أما إذا كان الدليل الرقمي غير المشروع دليل براءة فإن الأمر فيه إختلاف، و يمكن رد ذلك إلى ثلاث إتجاهات:

-الأول يرى أن المشروعية لازمة في كل دليل سواء أكان دليل إدانة أم براءة، و إثبات البراءة كالإدانة لا يكون إلا من دليل تم الحصول عليه من خلال سبل مشروعة ولا يصح أن يفلت إثبات البرءاة من قيد المشروعية الذي هو شرط أساسي في أي تشريع.

- والإتجاه الثاني يرى أن المشروعية لازمة في أدلة الإدانة دون البراءة لأن الأصل في الإنسان البراءة ولا حاجة لإثباتها.

- أما الإتجاه الثالث فيرى أن أدلة البراءة غير المشروعة يمكن الأخذ بها وقبولها في حالات دون أخرى طالما أنه تم الحصول عليها بوسائل لا تصل إلى حد الجريمة، وإنما تتضمن مخالفة قاعدة إجرائية إذ يمكن في هذه الحالة الإستناد إلى هذه الأدلة.

والراجح من بين هذه الإتجاهات هو الإتجاه الذي يقصر المشروعية على دليل الإدانة دون البراءة لأن عدم قبول دليل البراءة بحجة أنه غير مشروع يؤدي إلى نتيجة خطيرة وهي إمكانية إدانة بريء وهو ما لا يستقيم عدلا ولا منطقا.

المطلب الثاني: حجية الدليل الرقمي في إطار نظـــرية الإثبات الجنائي

إن مسألة تقيم الدليل الجنائي في إثبات الواقعة الجرمية هي مسألة موضوعية محضة، للقاضي أن يمارس سلطته التقديرية فيها، لأجل هذا فالسائد في الفقه الجنائي أن القاضي الجزائي له الحرية في تقدير الأدلة الجنائية وتكوين قناعته،وأن يبني حكمه على أي دليل متى إطمأن إليه حتى ولو كان هذا الدليل مستمدا من محاضر جمع الإستدلالات(1).

ولا يشترط أن يكون الدليل الذي يستند إليه القاضي صريحا دالا على الواقعة المراد إثباتها بل يكفي أن يكون إستخلاصها إستنتاجا من الظروف والقرائن وترتيب النتائج على المقدمات. وأدلة

(1)محمد عيد الغريب، حرية القاضي الجنائي في الإقتناع اليقيني و أثره في تسبيب الأحكام، ص32.

الدعوى تخضع في كل الأحوال لتقدير القاضي ما دام هذا الدليل غير مقطوع بصحته،[1]، ويترتب على ذلك أن الأدلة الجزائية لا تحظ أمام القاضي الجزائي بقوة حاسمة في الإثبات، وعلى هذا الأساس فكما يصح للقاضي أن يؤسس إقتناعه على أي دليل يصح له أيضا أن يهدره.لكن في المقابل لا تعني حرية القاضي في الإقتناع التحكم المطلق بل إن القاضي يلتزم بأن يتحرى المنطق الدقيق في تفكيره الذي قاده إلى إقتناعه، ففي الوقت الذي منح فيه القانون للقاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقا لإقتناعه الشخصي وفتح أمامه باب الإثبات على مصراعيه كي يستلهم عقيدته من أي موطن يراه فإنه في المقابل لم يطلق له العنان ليقضي كيفما شاء أو أراد وفقا لمزاجه الشخصي وحسب أهوائه بل لقد أحاطه بسياج من القيود والضوابط التي تشكل في مجموعها شروطا لإعمال المبدأ وتطبيقه التطبيق الأمثل بما يضمن الوصول إلى الحقيقة الفعلية دون الإفتئات على الحقوق والحريات.

إلا أن تطبيق ذلك على الدليل الرقمي قد يثير بعض الصعوبات، فالقاضي بثقافته القانونية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الرقمي، فضلا عن تمتع هذا الدليل من حيث قوته التدليلية بقيمة إثباتية قد تصل إلى حد اليقين شأنه في ذلك شأن الأدلة العلمية عموما، ومن جهة أخرى فإن الطبيعة الفنية الخاصة بالدليل الرقمي تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكونبمقدور غير المتخصص إدراك ذلك العبث، ومع نقص الثقافة المعلوماتية للقاضي الجزائي فهل عليه التوسع في سلطته عند تقدير الدليل لتمتد وتشمل الدليل الرقمي، وهل يمكن التسليم بخضوع الدليل الرقمي للمناقشة والبحث في مصداقيته لقبوله أو طرحه لعدم الإقتناع به.

وعلى هدي ما سبق طرحه فإننا سوف نناقش ما هي الشروط التي يجب أن يتوافر عليها الدليل الرقمي حتى يعبر عن حقيقة علمية ثابتة (الفرع الأول) ومدى تأثير ذلك على مبدأ الإقتناع الشخصي للقاضي الجزائي (الفرع الثاني).

الفرع الأول: شروط قبول الدليل الرقمي:

مما لاشك فيه أن الدليل الرقمي ما هو إلا تطبيق من تطبيقات الدليل العلمي بل وأكثر منه حجية في الإثبات وذلك بما يتميز به من موضوعية وحياد وكفاءة، وهو محكم وفق قواعد علمية حسابية قاطعة لا تقبل التأويل، مما يقوي من يقينيته ويساعد القاضي في التقليل من الأخطاء

---

[1] أشرف عبد القادر قنديل، النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي، المرجع السابق ص235.

القضائية والإقتراب أكثر إلى تحقيق العدالة والتوصل بدرجة أكبر نحو الحقيقة، ذلك أن التقنية العلمية قد توفر طرقا دقيقة لجمع الأدلة تتمتع بقوة علمية يصعب إثبات عكسها.لكن إذا كان صحيحا أن الدليل الرقمي وبحكم طبيعته العلمية يمثل أخبارا صادقا عن الواقع بإعتبار علميته وموضوعيته وحياده وكفاءته، إلا أن هذا لا ينف إستبعاد كونه موضع شك من حيث سلامته من العبث من ناحية وصحة الإجراءات المتبعة في الحصول عليه من ناحية أخرى، إذ يمكن أن يشكك في سلامة الدليل الرقمي من ناحيتين :

-الأولى:إمكانية خضوعه للعبث ولخروج به على نحو يخالف الحقيقة، إذ يقدم هذا الدليل معبرا عن واقعة معينة صنع أساسا لأجل التعبير عنها خلافا للحقيقة، دون أن يكون في إستطاعة غير المتخصص إدراك ذلك العبث على نحو يمكن معه القول أن ذلك قد أصبح هو الشأن بالنسبة لأغلب الأدلة الرقمية التي تقدم للقضاء، ذلك أن التقنية الحديثة تمكن من العبث بالدليل الرقمي بسهولة بحيث يظهر وكأنه نسخة أصلية في تعبيره عن الحقيقة.

- والثانية تتعلق بنسبة الخطأ في الحصول على الدليل الرقمي وذلك راجع إما للخطأ في إستخدام الأداة المناسبة في الحصول على الدليل الرقمي كالخلل في الشفرة المستخدمة أو إستخدام مواصفات خاطئة، وإما الخطأ في إستخلاص الدليل بسبب إستخدام أداة تقل نسبة صوابها عن 100% وهذا ما يحدث غالبا في وسائل إختزال المعطيات أو معالجتها بطريقة تختلف عن الطريقة الأصلية التي تم تقييمها.

وعلى هذا الأساس فإن الشك في الدليل الرقمي لا يتعلق بمضمونه وإنما بعوامل مستقلة عنه لكنها تؤثر في مصداقيته، لذلك فإن الأمر يتطلب وجوب توافر مجموعة من الشروط[1]في الدليل الرقمي من أجل إقترابه نحو الحقيقة وقبوله كدليل في الإثبات الجنائي،تُشيد عليه الحقيقة في الدعوى الجنائية سواء بالإدانة أو البراءة.

([1])نصت بعض التشريعات المقارنة على بعض الشروط والضوابط التي يجب مراعاتها في مخرجات الحاسب الآلي لكي يمكن قبولها كأدلة إثبات من أهمها أن يتم تحدد هوية الشخص أو الجهة المنسوب لها هذه المخرجات بصورة قاطعة وأن يتم إستخلاص المعلومات المخزنة إلكترونيا وحفظها بصورتها الأصلية التي أنشئت عليها وبصورة تضمن عدم تعرضها لأي شكل من أشكال العبث والتلف وهذا الشرط يتطلب إتخاذ بعض الإجراءات من أهمها التحقق من سلامة الحاسب الآلي ودقته في عرض المعلومات المخزنة وحفظ مخرجات الحاسب الآلي وتخزينها في بيئة مناسبة وكفاءة ونزاهة القائمين على جمع الأدلة وتخزينها.

أولا: وجوب يقيـــنية الأدلة الرقمية و غير قابلتها للشك: يشترط في الأدلة المستخرجة من المنظومة المعلوماتية والأنترنات أن تكون غير قابلة للشك حتى يمكن الحكم بموجبها بالإدانة ذلك أنه لا مجال لدحض قرينة البراءة أو إفتراض عكسها إلا عندما يصل إقتناع القاضي إلى حد الجزم واليقين،[1] ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الرقمية على إختلاف أشكالها التي تتوافر عن طريق الوصول المباشر إليها أو بمجرد عرضها كمخرجات على شاشة الحاسوب، ويستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية (رقمية) وما ينطبع في ذمته من تصورات وإحتمالات بالنسبة لها أن يحدد قوتها الإستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه، وكذا الوصول إلى يقينية هذه المخرجات عن طريق المعرفة الحسية التي تدركها الحواس من خلال معاينته لهذه المخرجات وفحصها، وكذا عن طريق المعرفة العقلية من خلال ما يقوم به من إستقراء وإستنتاج ليصل إلى الحقيقة التي يهدف إليها ويجب أن يصدر حكمه إستنادا إليها.[2]

ويشترط قانون البوليس والإثبات البريطاني لسنة 1984 حتى تتحقق يقينية الأدلة الرقمية أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة، وفي كندا فإن الرأي السائد في الفقه هو إعتبار مخرجات الحاسوب من أفضل الأدلة لذا فإنها تحقق اليقين المنشود في الأحكام الجزائية. وقد نصت بعض القوانين في الولايات المتحدة الأمريكية أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد من أفضل الأدلة المتاحة للإثبات وبالتالي يتحقق مبدأ اليقين لهذه الأدلة، وتنص القواعد الفدرالية على أن الشرط الأساسي للتوثيق أو التحقق من صحة أو صدق الدليل كشرط مسبق لقبوله هو أن يفي بأمارة أو بينة كافية لأن تدعم الوصول إلى الأسرار التي تتصل بالموضوع بما يؤيد المطالبة المدعى بها.[3]

ويتحقق اليقين للأدلة الرقمية أكثر بإخضاعها للتقييم الفني بوسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وكذا صحة الإجراءات المتبعة في الحصول عليه من أجل تفادي تلك العيوب التي قد تشوبه، فمثلما يخضع الدليل الرقمي لقواعد وإجراءات معينة تحكم

([1])علي حسن محمد الطوالبة، المرجع السابق، ص190، مرجع سابق.

([2])هلالي عبد اللاه أحمد، حجية المخريات الكومبيوترية في المواد الجنائية، المرجع السابق،، ص91 .

([3]) علي حسن محمد الطوالبة، المرجع السابق ص191.

طرقالحصول عليه فإنه يخضع لقواعد أخرى للحكم على قيمته التدليلية من الناحية العلمية وذلك راجع للطبيعة الفنية لهذا الدليل.(1)وتتمثل وسائل تقييم الدليل الرقمي في:

1/تقييم الدليل الرقمي للتحقق من سلامته من العبث: ويمكن التأكد من سلامة الدليل الرقمي من وقوع العبث به بعدة طرق أهمها:

- فكرة التحليل التناظري الرقمي والتي من خلالها يتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثم يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا.(2)ويستعان في ذلك بإستخدام علم الكومبيوتر الذي يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون وكينونة الدليل الرقمي، وهذا العلم يستعان به أيضا في كشف مدى التلاعب بمضمون هذا الدليل.

- إستخدام عمليات حسابية خاصة تسمى الخوارزميات ويلجؤ إلى هذه التقنية في حالة عدم الحصول على النسخة الأصلية للدليل الرقمي، أو في حالة أن العبث قد وقع على النسخة الأصلية إذ بالأمكان التأكد من سلامة الدليل الرقمي من التبديل والتحريف والتغيير بإستعمال هذه العمليات الحسابية.

- إستعمال الدليل المحايد وهو نوع من الأدلة الرقمية المخزون في البيئة الإفتراضية لا علاقة له بموضوع الجريمة، ولكنه يساعد في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول أي تعديل عليه في النظام الكومبيوتري.(3)

ولا شك أن الخبرة التقنية تحتل في هذه الحالة دورا مهما في التثبت من سلامة الدليل الرقمي فإذا كان للخبرة التقنية أهمية كبرى في مجال إستخلاص الدليل الرقمي،فإن لها ذات الدور في بحث مصداقيته وتقييمه من حيث عدم حصول أي عبث عليه، فنقص الثقافة المعلوماتية للقاضي الجزائي قد يحتم وكواجب قضائي أن يستعين في هذه المسائل بوسائل الخبرة كنهج ليس من أجل إستقاء الدليل فحسب، بل لبحث مصداقيته في مجال المعالجة الآلية للمعلومات وتحقيق اليقينية لهذا الدليل.

2/تقييم الدليل الرقمي من حيث السلامة الفنية للإجراءات المستخدمة في الحصول عليه:

(1)خالد عباد الحلبي، إجراءات التحري في جرائم الحاسوب والأنترنات، المرجع السابق.ص249

(2)طارق محمد الجملي، المرجع السابق، بدون ترقيم.

(3)ممدوح عبد الحميد عبد المطلب، المرجع السابق.ص47-22

سبق الحديث على أن الدليل الرقمي يتم الحصول عليه بإتباع جملة من الإجراءات الفنية والتي من الممكن أن يعتريها خطأ قد يشكك في سلامة نتائجها، الأمر الذي يحتم إخضاعها إلى إختبارات(1)كوسيلة للتأكد من سلامة هذه الإجراءات من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات، ويتبع في ذلك مجموعة من الخطوات أهمها:

-إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج ويكون ذلك بإتباع إختبارين أساسيين يتم التأكد من خلالهما أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الرقمي وفي ذات الوقت لم نضف إليها أي بيان جديد، وهو ما قد يعطي للنتائج المقدمة مصداقية في التدليل على الواقع، ويتمثل هذان الإختباران في: إختبار السلبيات الزائفة ومفاده أن تخضع الأداة المستخدمة في الحصول على الدليل لإختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي وأنه لم يتمإغفال معطيات مهمة عنه. أما الإختبار الثاني والذي يعرف بإختبار الإيجابيات الزائفة فمفاده إخضاع الأداة المستخدمة في الحصول على الدليل الرقمي لإختبار يمكن من التأكد من أن هذه الأداة لا تعرض معطيات إضافية جديدة.

-الإعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل، إذ تبين الدراسات العلمية والبحوث المنشورة في مجال تقنية المعلومات الطرق السليمة التي يجب إتباعها في الحصول على الدليل الرقمي وفي المقابل بينت تلك الدراسات أيضا الأدوات المشكوك في كفاءتها وهو ما يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات.

---

(1)تعرف هذه الإختبارات بإختبارات (داوبورت) وذلك نسبة للحكم الذي أصدرته المحكمة العليا الأمريكية في قضية داويورت ضد ميريل للصناعات الدوائية سنة 1993.

ثانيا: وجوب مناقشة الأدلة الرقمية المستخرجة من الحاسوب:إن حرية الدليل الجنائي مشروطة بأن يكون الدليل الذي يستند إليه القاضي قد طرحت مناقشته بالجلسة، ويكون كذلك متى كان له أصل ثابت في أوراق القضية المطروحة على القاضي،(1) وهو ما يجعل هذهالأدلة متاحة للخصوم لكي يتمكن كل خصم من إعداد دفاعه فإن كان الدليل في صالحه يدافع عنهوإن كان ضده يشك فيه وبضعفه. ولا يمكن للقاضي حينئذ أن يؤسس إقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحكمة وخضعت لحرية مناقشة أطراف الدعوى.

وهذا يعني أن الأدلة الرقمية المتحصلة لإثبات الجرائم المعلوماتية سواء كانت مطبوعة أم إتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مصورات فلمية، كلها ستكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال البيئة الإلكترونية يجب أن يعرض في جلسة المحكمة ليس من خلال ملف الدعوى في التحقيق الإبتدائي وإنما يعرض بصفة مباشرة أمام القاضي.

وهذه الأحكام تنطبق على كافة الأدلة المتولدة من الحاسبات الإلكترونية فبالنسبة لشهود الجرائم المعلوماتية(2)الذين يكون قد سبق سماعهم في التحقيق الإبتدائي فإنه يجب أن يتم إعادة سماعهم مرة أخرى من جديد أمام المحكمة، كذلك بالنسبة لخبراء المعلوماتية على إختلاف تخصصاتهم ينبغي أن يمثلوا أمام المحكمة لمناقشتهم ومناقشة تقاريرهم التي خلصوا إليها.

ويترتب على هذا المبدأ أن القاضي لا يمكنه أن يحكم في الجرائم المعلوماتية بناءا على علمه الشخصي أوإستنادا إلى رأي الغير إلا إذا كان الغير من الخبراء وقد إرتاح ضميره إلى التقرير المحرر من قبله فقرر الإستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه.

والحديث في هذه المسألة يجرنا إلى مناقشة مدى تأثير الأصالة الرقمية(3)للدليل الرقمي على مبدأ قبوله من طرف القضاء، إذ تبرز هذه المشكلة بصورة جلية عندما يقوم المتهم بإزالة الدليل

---

(1)أحمد فتحي سرور الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، 1996ص392.

(2)الشاهد المعلوماتي هو الفني صاحب الخبرة والمتخصص في تقنية علوم الحاسب الآلي والذي تكون لديه معلومات جوهرية لولوج نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله.

(3) هناك تمييز حقيقي بين الأصالة للدليل في طابعها المادي وبين الأصالة في طابعها الرقمي من حيث أن الأولى إن هي سوى تعبير عن وضعية مادية ملموسة كما هو الشأن في الورق المكتوب أو بصمة الأصبع أو الحدوث العيني للواقعة في حين أن الثانية ليست سوى تعداد غير محدود لأرقام ثنائية موحدة في الصفر الواحد.

الرقمي عند بعد، فيكون ما تبقى منه هو مجرد نسخة فقط يتم التوصل إليها عن بعد أيضا بطرق المراقبة الإلكترونية مثلا، ومن ثم فالسؤال هنا هل يكفي ناتج المراقبة الإلكترونية وحده للقول بأن الدليل هنا هو دليل أصلي وبالتالي يقبل طرحه على القضاء ومناقشته ضمن أدلة الدعوى وذات السؤال ينطبق على حالة الدليل المسترد بعدما تم حذفه بإستخدام خاصية الإلغاء.

إن مناقشة هذه المسألة من الناحية القانونية دفع بالتشريع المقارن أن يعتمد منطق إفتراض أصالة الدليل الرقمي، حيث نص قانون الإثبات الأمريكي في المادة (3/1003) أنه إذا كانت البيانات المخزنة في حاسوب أو آلة مشابهة فإن أي مخرجات طابعة منها أو مخرجات مقروءة تبرز إنعكاسا دقيقا للبيانات و تعد بيانات أصلية. وتبرز أهمية التسليم بمنطق إفتراض الأصالة في الدليل الرقمي على المستوى القانوني ذلك أن الطبيعة التقنية للدليل الرقمي لا تعبر عن قيمة أصلية بمجرد رفع محتواه من النظام المعلوماتي إذ يبقى متواجدا في كل مكان يتم إستدعاؤه منه.(1)

وعلى هدي ما سبق فإن هناك من يذهب إلى الإعتقاد بأنه بمقدار إتساع مساحة الأدلة العلمية بمقدار ما يكون إنكماش وتضاؤل دور القاضي الجزائي في التقدير، خاصة أمام غياب الثقافة المعلوماتية للقاضي وقد يُستتبع ذلك بالقول أن التطور العلمي من شأنه أن يطغى على نظام الإقتناع القضائي ولا يبقى للقاضي سوى الإذعان لرأي الخبراء المختصين دون أي تقدير من جانبه فمثل هذا الأمر يدفعنا إلى بحث مدى تأثير القيمة العلمية للدليل الرقمي على مبدأ إقتناع القاضي الجزائي.

الفرع الثاني: أثر القيمة العلمية للدليل الرقمي في مجال الإثبات الجنائي

لقد تعاظم دور الإثبات العلمي مع بروز الدليل الرقمي إلى حقل الأدلة الجنائية كأفضل دليل لإثبات الجرائم المعلوماتية، مما ألزم القاضي أن يتعامل معه في مقابل نقص الثقافة المعلوماتية من جهة وشروط السلامة التي يتمتع بها من العبث والخطأ من جهة أخرى، فهل من شأن ذلك أن للقاضي يسلم ويبني إقتناعه بالدليل الرقمي على أساس أن أمره محسوم علميا؟

يرى البعض(2)أنه ليس بشرط أن يكون إقتناع القاضي يقينيا وذلك حسب المفهوم القضائي له ويبررون ذلك بأن القاضي لا يملك وسائل إدراك اليقين كحالة ذهنية تلتصق بالحقيقة دون أن

---

(1)محمد بوبكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنات، مرجع سابق. ص973،

(2)أنظر د.محمد زكي أبو عامر، الاجراءات الجنائية، دار الجامعة الجديدة ،طبعة 2008 ،ص813-814.

تختلط بأي شك على المستوى الشخصي أو بجهل أو غلط على المستوى الموضوعي، كما أن الإقتناع ليس إعتقادا لأن القاضي لا يجوز أن يحكم بناءا على أسباب شخصية صلحت لحمله هو نفسه على التسليم بثبوت الوقائع، لكنها تصلح إذا نظر إليها من الناحية الموضوعية من جانب الآخرين.[1] وينتهي أصحاب هذا الإتجاه إلى أن الإقتناع يقف موقفا وسطا بين اليقين والإعتقاد ويؤكدون أن الإقتناع ليس يقينا وليس جزما بالمعنى العلمي لليقين والجزم كحالة موضوعية لا تورث شكا لدى من تيقن أو جزم ولا جهلا ولا غلطا لدى الآخرين، وإنما الإقتناع هو إعتقاد قائم على أدلة موضوعية يقوم على إستقراء وإستحياء الأدلة التي يتوجه بها أطراف الخصومة لنيل إقتناع القاضي.

ويقصد بالدليل العلمي تلك النتيجة التي تسفر عليها التجارب العلمية لإثبات أو لنفي الواقعة التي يثار الشك بشأنها، وغالبا ما يتطلب فهمها معرفة ودراية خاصة قد لا يملكها القاضي بحكم تكوينه القانوني المحض، والدليل الرقمي بوصفه تطبيقا من تطبيقات الدليل العلمي لا يمكن للقاضي أن ينازع في قيمة ما يتمتع به من قوة إستدلالية قد إستقرت بالنسبة له وتأكدت من الناحية العلمية.

فإذا كان للقاضي في الدليل سلطة تقديرية واسعة في اللجوء إلى الخبرة وتقدير قيمتها الإثباتية إنطلاقا من مبدأ حرية الإثبات في المواد الجزائية والذي تولد عنه مبدأ القاضي خبير الخبراء فإن ذلك مقتصر على ما يمكن للقاضي أن يبت فيه لوحده، أما المسائل ذات الصبغة الفنية البحتة فلا يجوز للقاضي أن يحل نفسه فيها محل الخبير ولا يمكنه طرح رأيه إلا لأسباب سائغة ومقبولة، إذ يذهب في هذا الصدد إتجاه عريض من الفقه الجنائي إلى القول أن الأدلة الرقمية تتمتع بحجية قاطعة في الدلالة على الوقائع التي تتضمنها، وأنه يمكن التغلب على مشكلة التشكيك في مصداقيتها من خلال إخضاعها لإختبارات تمكن من التأكد من صحتها وسلامتها، وأنه لا يجب الخلط بين الشك الذي يشوب الدليل الرقمي بسبب إمكانية العبث به أو لوجود خطأ في الحصول عليه، وبين القيمة الإقناعية لهذا الدليل، فالحالة الأولى لا يملك القاضي الفصل فيها لأنها مسألة فنية والقول فيها هو قول أهل الخبرة، فإن سلم الدليل الرقمي من العبث والخطأ وتوافرت فيه الشروط المذكورة سابقا فإنه لن يكون للقاضي سوى القبول بهذا الدليل ولا يمكنه رده أو التشكيك في قيمته التدليلية لكونه

[1]عفيفي كامل عفيفي، المرجع السابق، ص384.

وبحكم طبيعته الفنية يمثل أخبارا صادقا عن الوقائع، ما لم يثبت عدم صلة هذا الدليل بالجريمة المراد إثباتها، لذلك يرى هذا الإتجاه أن الدليل العلمي ومنه الدليل الرقمي أصبح يقيد حرية القاضي في تقدير الدليل ويجبره على الحكم بمقتضاه ولو لم يكن مقتنعا بصحة الواقعة المطروحة أمامه، إذ لم يعد القاضي الجزائي وفقا لهذا الإتجاه حرا في وزن وتقدير الدليل العلمي الذي بات يأخذ دور الصدارة في الإثبات الجنائي خاصة بعد ظهور الأدلة الرقمية وإنشاء المعامل الجنائية لفحص هذه الأدلة وتقييمها.

لكن ثمة رأي آخر يرى أن الوسائل العلمية في أغلب حالاتها ليست دليلا مستقلا في ذاته وإنما هي قرائن يتم دراستها لإستخلاص دلالتها وهي غير مستقلة عن القرائن، ومؤدى ذلك أنها لا تصلح في ذاتها كدليل وحيد في الإثبات الجنائي، وأنه إذا كان يتعين على القاضي الإستعانة بأهل الخبرة في المسائل الفنية البحتة وأن يعتمد على رأيهم فيما يتعلق بهذه المسائل، إلا أنه من غير المقبول أن يتخلى القاضي عن حقه إذا رأى لأي سبب من الأسباب ألا يأخذ برأي الخبير كأن يتبين له بأن الدليل الرقمي لا يتفق مع الظروف والملابسات التي وجد فيها، فهي ما يدخل في نطاق تقديره الذاتي ومن صميم وظيفته القضائية.

ذلك أن مجرد توافر الدليل العلمي الرقمي لا يعني أن القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أو البراءة، فالدليل الرقمي ليس آلية معدة لتقرير إقتناع القاضي بخصوص مسألة غير مؤكدة.(1)فحسب هذا الإتجاه أنه مهما علا شأن الأدلة العلمية والرقمية في مسألة الإثبات الجنائي فإنه يجب أن نبقي على سلطة القاضي التقديرية في تكوين إقتناعه من هذه الأدلة وذلك من أجل ضمان تنقية هذه الأدلة من شوائب الحقيقة العلمية، ويظل القاضي هو المسيطر على هذه الحقيقة لأنه من خلال سلطته التقديرية يستطيع أن يفسر الشك لصالح المتهم وأن يستبعد الأدلة التي يتم الحصول عليها بطرق غير مشروعة وضرورية أكثر من أجل جعل الحقيقة العلمية قضائية.

---

(1)جميل عبد الباقي الصغير ، المرجع السابق، ص22.

المطب الثالث: موقف المشرع الجزائري من الدليل الرقمي فـــيمجـــال الإثبات الجزائي

إن الإثبات في المواد الجنائية هو النتيجة التي تتحقق باستعمال وسائله وطرقه المختلفة للوصول إلى الدليل الذي يستعين به القاضي لإستخلاص حقيقة الوقائع المعروضة عليه و إعمال حكم القانون عليها، ويعني ذلك أن موضوع الإثبات هو الوقائع وليس القانون.[1]

وبالتالي فإن الإثبات الجزائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل ووجود الدليل على ذلك، ويعتبر الدليل الوسيلة القانونية التي يستيعن بها القاضي للوصول إلى الحقيقة وكشف غموض الجريمة ونسبتها إلى المتهم.

ولقد ذهب الفقه الإجرائي إلى وضع نظامين إجرائين في مجال الإثبات الجزائي يختلفان فيما بينهما من حيث الأسس التي يقوم عليها كل واحد منهما وهذه الأنظمة هي:

-نظام الإثبات القانوني أو المقيد وفيه يحدد القانون الأدلة التي يجوز الأخذ بها والإستناد عليها والثاني هو نظام الإثبات الحر أو المطلق وفيه لا يقيد القانون القاضي بأدلة معينة في إثبات الواقعة وله أن يقتنع بأي دليل يعرض عليه.

فأي من هذين النظامين أخذ الشرع الجزائري وما أثر ذلك على مسألة الإثبات بالدليل الرقمي في الجريمة المعلوماتية.

الفرع الأول: أنظـــمة الإثبات الجـــزائي

يوجد في مجال الإثبات الجزائي نظامان:

أولا: نظام الإثبات المقيد أو نظام الأدلة القانونية:Systémedela preuve légaleمفاد هذا النظام هو أن يتقيد القاضي في حكمه سواء بالإدانة أو البراءة بأنواع معينة من الأدلـــــة طبقا لما يرسمه التشريع، فالفكرة الأساسية لهذا النظام تقوم على أن المشـــرعهو الذي يكـــون له الدور الأساسي في الإثبات، وذلك من خلال التحديد المسبق للأدلة المقدمة في الدعـــوى والـــتي يستند إليها القاضي الجزائي في حكمه ولا سبيل له إلى الإستناد إلى أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات.

([1])أشرف عبد القادر قنديل النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي، المرجع السابق، ص212.

وفي هذا النظام لا يكون للقاضي الجزائي دور في تقدير القيمة الإقناعية للدليل فيتقيد القاضي وفق هذا النظام بالأدلة التي رسمها الشرع سلفا دون أن يُعمل فيها ميوله أو إقتناعه الشخصي بشأنها، إذ يقوم إقتناع الشرع مقام إقتناع القاضي وعليه فإن اليقين القانوني يقوم أساسا على إفتراض صحة الدليل بغض النظر عن حقيقة الواقع وإختلاف ظروف الدعوى، ويتجلى دور القاضي في هذا النظام كمطبق فحسب من حيث مراعاة توافر الدليل وشروطه، بحيث إذا لم تتوافر هذه الشروط وتلك الآليات التي يتطلبها القانون في الدليل فإن القاضي لا يستطيع أن يحكم بالإدانة حتى ولو كان إقتناعه يقينيا بإرتكاب المتهم للجريمة المسندة إليه.

ويقوم هذا النظام على مجموعة من الخصائص أهمها أن دور القاضي الجزائي سلبي، ذلك أن الإثبات الجنائي في هذا النظام يخضع لقواعد شكلية تتضح في سلطة القاضي المقيدة في تقدير عناصر الإثبات التي يستمد منها إقتناعه وتقدير قيمة الأدلة المعروضة عليه، كما يتميز أيضا هذا النظام بالدور الإيجابي للمشرع في عملية الإثبات من حيث أنه هو الذي ينظم قبول الأدلة سواء عن طريق تعيين الأدلة المقبولة للحكم بالإدانة، أو بإستبعاد أدلة أخرى أو بإخضاع كل دليل لشروط معينة، وأنه هو الذي يحدد القيمة الإقناعية لكل دليل بأن يعطي لبعض الأدلة الحجية الأقوى دون الأدلة الأخرى.

وقد أعاب الفقه الجنائي على هذا النظام أنه أخرج القاضي من وظيفته الطبيعية التي تتمثل في فحصة للدليل وتقديره، ومن ثم تكوين إقتناعه الشخصي وأقحم المشرع في وظيفة القاضي وإملاء أدلة الإدانة عليه على سبيل الحصر.

ومن العيوب التي واجهها هذا النظام أيضا أنه قام بتقنين اليقين في نصوص قانونية محددة سلفا رغم أن اليقين مسألة يطرحها الواقع ويقدرها القاضي.

ثانيا: نظام الإثبات الحر أو نظام الإقتناع الشخصي للقاضي الجزائي:وفقا لهذا النظام لا يرسم القانون طرقا محددة للإثبات، إذ يتمتع القاضي الجزائي في هذا النظام بحرية مطلقة في تكوين إعتقاده من أي دليل يُطرح أمامه.(1)ومن ثمة فإن هذا النظام يقوم على خاصيتين أساسيتين:

(1)محمد عيد الغريب حرية القاضي الجنائي في الإقتناع اليقيني وأثره في تسبيب الأحكام،المرجع السابق، ص8.

-الأولى تتمثل في إطلاق حرية الإثبات للقاضي الجزائي إنطلاقا من موضوع الإثبات في المسائل الجزائية يتعلق بوقائع مادية ونفسية لا يصلح لإثباتها تحديد مجموعة من القواعد الإثباتية مسبقا، بل إن الإثبات في هذه المسائل يكون بكافة طرق الإثبات.

- والخاصية الثانية تتمثل في حرية القاضي الجزائي في الإقتناع بالدليل المطروح عليه في جلسة المحاكمة دون أن يكون عليه أي رقيب سوى ضميره ودون أن يكون مطالبا ببيان سبب إقتناعه بدليل دون آخر.

وعلى هذا الأساس يكون للقاضي الجزائي دور فعال حيال الدليل الذي يوضع أمامه، وله في مقابل ذلك كافة الصلاحيات التي تمكنه من إتخاذ الإجراء الذي يراه مناسبا ويخدم إظهار الحقيقة.

وعقيدة القاضي هي نتاج وزن الأدلة المطروحة بالدعوى الجزائية أمامه والذي يقوم بقبول الأدلة التي قدمها أطراف الدعوى، فلا يوجد حظر على أدلة إلا إذا كانت غير مشروعة. وقد ذهب البعض[1]إلى القول أن الإقتناع الشخصي للقاضي الجزائي هو الضمانة الحقيقية لضبط ميزان العدالة.

الفرع الثاني:موقف الشرع الجزائي الجزائري من أنظمة الإثبات وأثر ذلك في إثبات الجريمة المعلوماتية.

نصت المادة 212 من قانون الإجراءات الجزائية على أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات وللقاضي أن يصدر حكمه تبعا لإقتناعه الخاص...." كما نصت المادة 307 من قانون الإجراءات الجزائية أيضا أن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين إقتناعهم وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة للمتهم...."

ومن خلال هذين النصين القانونيين يتضح جليا أن المشرع الجزائري قد تبنى كقاعدة عامة نظام الإقتناع الشخصي للقاضي الجزائي، إلا واستثناء نجده أخذ أيضا بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط لإثباتها أدلة قانونية محددة مسبقا وعلى سبيل الحصر[2].

([1])أشرف عبد القادر قنديل، المرجع السابق، ص213.

(2) أنظر المادتين 339،341 من قانون العقوبات الجزائري

وبتحليل المادة 212 من قانون الإجراءات الجزائية نجدها تكرس قاعدتين تكمل إحداهما الأخرى، قاعدة الإقتناع الحر للقاضي الجزائي من جهة وقاعدة حرية إختيار وسائل الإثبات الجزائي من جهة أخرى.

وإذا كان الدليل الرقمي ذو الأصالة العلمية هو الأوفر والأنسب في إثبات الجريمة المعلوماتية فما مدى إمكانية إعمال القاضي الجزائي لمبدأ الإقتناع الشخصي حيال هذا الدليل طبقا لأحكام المادة 212 من قانون الإجراءات الجزائية.

أولا: مفهوم الإقتناع الشخصي للقاضي الجزائي:إن الإقتناع الشخصي للقاضي الجزائي هو عبارة عن نشاط عقلي لا يتدخل المشرع ليبين للقاضي كيفية ممارسته و ترجمته إلى واقع منتج ولا يرسم له كيف يشكل معادلاته الذهنية في مجال تقدير الأدلة ليصل من خلالها إلى الحقيقة.

1/تعريف مبدأ الإقتناع الشخصي:يعرف فقهاء القانون الجنائي الإقتناع بأنه حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث، أو بمعنى آخر هو حالة ذهنية ذو خاصية ذاتية نتيجة تفاعل ضمير القاضي وأدلة الإثبات المطروحة والتي يثيرها الخصوم إما لإثبات أو إنكار إتهام.[1]كما عُرف الإقتناع الشخصي أيضا بأنه حالة ذهنية ذاتية تنجم عن إمعان الفكر في وقائع معروضة من أجل بحثها والوصول بعد ذلك إلى حالة تطرد الشك والإحتمال، ويجد هذا المبدأ مناخه الطبيعي الملائم في ظل مذهب الإثبات الحر الذي لا يضع تقديرا مسبقا لأدلة معينة لا يمكن الوصول بغيرها إلى اليقين.[2]ومن خلال هذا التعريف فإن الإقتناع الشخصي للقاضي الجزائي يتميز بخاصيتين هما:

-أنه حالة ذهنية مبنية على الإحتمال وأن العبرة ليست بكثر الأدلة وإنما بما تتركه من أثر في نفسية القاضي، لأن هذا التأثير سيلعب دورا في تحديد مصير الدعوى الجزائية بالإدانة أو البراءة.

- والخاصية الثانية تتمثل في أن القاضي حر في أن يأخذ عقيدته أو إقتناعه من أي دليل لكن يجب التأكيد هنا أن حرية الإثبات في المسائل الجزائية ليست خاصية يتميز بها القاضي الجزائي

(1)نصر الدين ماروك، النظرية العامة للإثبات الجنائي، الجزء الأول، ص620.

(2)زبدة مسعود، الإقتناع الشخص للقاضي الجزائي، المؤسسة الوطنية للكتاب الطبعة الأولى، ص08.

لتتسع سلطته في الإدانة أو البراءة ولكنها، ترجع إلى أن الإثبات في المسائل الجزائية والوصول إلى الدليل مسألة جد صعبة وذلك لإختلاف أساليب إرتكاب الجريمة وأن المجرم عادة ما يسعى إلى إخفاء جريمته، لذلك فالبحث عن الحقيقة من خلال الأدلة الجزائية لا يكون إلا عن طريق منح القاضي الجزائي هامشا عن الحرية لمناقشة الدليل الذي يراه مناسبا في إثبات الجريمة.

2/وسائل تكوين الإقتناع الشخصي للقاضي الجزائي: إن الجهد الإستنباطي الذي يبذله القاضي من خلال نشاطه العقلي المكون لقناعته و الذي ينصرف إلى فرز الحقيقة من الدليل محل تقديرهيرتكز فيه القاضي على:

- قبوله جميع الأدلة المطروحة أمامه في الجلسة ولا يحظر على القاضي أو يفرض عليه دليل محدد ولا يتقيد إلا بقيد مشروعية الدليل وأنه قد تم طرحه للمناقشة بالجلسة.

- أن يقوم القاضي بوزن كل دليل على حدى عن باقي الأدلة المطروحة أمامه وله أن يهدر أي دليل مهما كانت قيمته طالما أنه لم يطمئن إليه.

- سلطة القاضي في تنسيق الأدلة المطروحة أمامه ومساندة الأدلة لبعضها أو ما يعرف بتساند الأدلة.

ثانيا: سلطة القاضي الجزائي في تقدير الدليل الرقمي:إن الأصالة العلمية للدليل الرقمي جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي، إذ أن هناك من يرى أن الدليل العلمي ومنه الدليل الرقمي له قوته الثبوتية الملزمة حتى للقاضي، مستندين في رأيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين وهناك من يرى أن مبدأ حرية القاضي في الإقتناع يجب أن يبسط سلطانه على كل الأدلة دون إستثناء حتى على الدليل الرقمي، معتبرين أن إعطاء الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى مذهب الإثبات القانوني (المقيد).والمشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الجرائم التي قد يتطلب إثباتها دليلا معينا، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين إقتناعه من أي دليل يطمئن إليه، فهل تنصرف هذه السلطة التقديرية التي يتمتع بها القاضي الجزائي إلى الدليل الرقمي المستخرج من الوسائل الإلكترونية؟

لقد سبق الذكر أن الجريمة المعلوماتية في القانون الجزائري تشمل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وكذا كل جريمة أخرى ترتكب أو يسهل إرتكابها بواسطة منظومة معلوماتية أو نظام للإتصالات الإلكترونية، وهذه الأخيرة قد تنصرف إلى جرائم تقليدية منصوص عليها في قانون العقوبات يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتية، وهذا يعني أن الإجرام المعلوماتي قد يأخذ وصف الجناية أو الجنحة أو المخالفة حسب وصف الجرم المرتكب بواسطة المنظومة المعلوماتية.وإن كان مبدأ الإقتناع القضائي عام النطاق لدى كافة أنواع

المحاكمالجزائية سواء كانت محاكم الجنايات أم الجنح أم المخالفات [1]،فإن قواعد بيان عناصر تقدير الدليل تختلف حسب إختلاف وصف الفعل المجرم. فإذا كان الفعل من طبيعة جنائية فإن محكمة الجنايات تتمتع بسلطة تقديرية مطلقة في مواجهة الأدلة المعروضة أمامها وتصدر أحكامها دون أن يكون قضاهَا مطالبين بتسبيب أحكامهم ولا رقابة لجهات الطعن عليهم.أما إذا أخذ الفعل المجرم وصف الجنحة فإن قاضي الجنح مطالب بعرض وبيان تقديره للدليل المعروض عليه من خلال تسبيب حكمه، والذي يكون محل رقابة من جهات الطعن،[2]لهذا فهو مطالب بإحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات والتي قد تأخذ شكل محاضر معدة بمناسبة تفتيش أو إعتراض مراسلات أو شكل تقرير خبرة محرر بمناسبة معاينة وفحص الأدلة المضبوطة من جهاز الإعلام الآلي أو دعامات إلكترونية.

فأما ما يتعلق بالمحاضر فإن الشرع إعتبر أنها كقاعدة عامة مجرد إستدلالات ما لم ينص القانون على خلاف ذلك، ولا يكون للمحضر أي قوة إثبات إلا إذا كان صحيحا من حيث الشكل، وأنه قد تم إعداده من طرف واضعه أثناء مباشرة أعمال وظيفته، ويكون مضمونه ما يدخل في إختصاصه.[3]إلا أن المحاضر التي يخول القانون لضباط الشرطة القضائية إعدادها بنص خاص لإثبات جنح معينة فإن هذه المحاضر تكون لها حجيتها ما لم يدحضها دليل عكسي.[4]

أما بالنسبة لتقارير الخبرة فإن المحكمة العليا ذهبت للقول أن الخبرة شأنها شأن باقي أدلة الإثبات تخضع للسلطة التقديرية لقاضي الموضوع،[5]وهذا المعنى تؤكده المادة 215 من قانون الإجراءات الجزائية التي تنص على أنه:" لا تعتبر التقارير المثبتة للجنايات أو الجنح إلا مجرد إستدلالات....".

(1)وإن كان المشرع الجزائري لم يحدد ذلك صراحة في المواد المقررة لهذا المبدأ راجع المواد 212 .307 من قانون الإجراءات الجزائية بخلاف المشرع الفرنسي فقد صرح ذلك صراحة حيث خصص المادة (353-1) من قانون الإجراءات الجزائية لتطبيق المبدأ أمام محكمة الجنايات كما نصت المادة (427) من ذات القانون على تطبيق هذا المبدأ بالنسبة لمحاكم الجنح.

(2)أنظر المادة 379 من قانون الإجراءات الجزائية الجزائري والتي تقابلها المادتين 485-593 من قانون الإجراءات الجزائية الفرنسي.

(3)أنظر المادة 214 من قانون الإجراءات الجزائية.

(4)أنظر المادة 216 من قانون الإجراءات الجزائية.

(5)ورد في مضمون قرار المحكمة العليا المؤرخ في 1995/07/11 المنشور في نشرة القضاء رقم 58 لسنة 2006، ص170.

لكن الطبيعة العلمية والتقنية للجريمة المعلوماتية غالبا ما تفرض على القاضي الإستناد في تكوين إقتناعه على الخبرة الفنية والتقيد بالنتيجة المتوصل إليها الخبير في تقرير خبرته ولا يمكنه طرحها وإستبعادها إلا إذا قدر أن ما تحمله من أدلة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة العلمية.فحسب الإجتهاد القضائي أنه أحيانا ما تكون الخبرة وحدها كافية بالنسبة للقاضي عندما يكون مطالبا للفصل في وقائع ذات طابع تقني دون أن يحتاج إلى مناقشتها.(1)

وفي الأخير يمكن القول أن إساءة استخدام التقنية المعلوماتية تعد من الموضوعات التي فرضت نفسها على المستوى الوطني و الدولي على حد سواء، وأجبرت التشريع الجزائي على التدخل من أجل مواجهتها بتشريعات حاسمة لمكافحتها ومعاقبة مرتكبيها.إلا أن ذلك يبدو غير كاف لتحقيق هذا الهدف فعلى المستوى الإجرائي تثير الجريمة المعلوماتية مشكلات عدة بدءامن مرحلة الإستدلال حتى صدور الحكم الجزائي لا سيما فيما يتعلق بإثبات الجريمة المعلوماتية ومدى صلاحية الدليـــل الرقمي للإثبات ومدى شرعية الأدلة المتحصل عليها عبر التقنية المعلوماتية وحجيتها أمام القـــاضي الجزائي، لذلك خُصص هذا الفصل لتناول هذه المسائل من خلال تحديد الأجهزة المكلفة بالبـــحث و التحري عن الجريمة المعلوماتية، ثم التعريف بالخصائص التي يتميز بها التحقيق و المحققـــون فيها، ثم بعد ذلك تم البحث في الدليل المناسب لإثبات هذا النوع من الجرائم وهو ما يعرف بالدليل الرقمي أين تم توضيح مفهومه وتحديد أشكاله ومصادر الحصول عليه، كما تم معالجة القواعد الإجرائية المستعملة في التحقيق من أجل استخلاصه وماهي الصعوبات و المعوقات التي تواجه القائمين على ذلك،كما تم التناول في هذا الفصل مسألة ضمانات المشتبه فيه أثناء ممارسة إجراءات الحصول على الدليل الرقمي وأثرها على الحق في الخصوصية، وأخيرا تم بحث القيمة القانونية للدليل الرقمي في مجال الإثبات الجزائي وما هو موقف المشرع الجزائري من هذا الدليل.

---

(1)قرار المحكمة العليا الغرفة الجنائية مؤرخ في 2002/06/04 نشرة القضاة رقم 58 لسنة 2006، ص255.

خـــاتمـــة

بعد أن فرغت من بسط مسائل الدراسة وسعيت إلى محاولة الإحاطة بجوانب البحث ضمن رؤية إجرائية تتناول مسألة البحث والتحري عن الجريمة المعلوماتية.

ووفاء لهذه الغاية كان لزاما علي الوقوف على تحديد الإطار القانوني للجريمة المعلوماتية، وهو الأمر الذي رصدته في الفصل الأول من هذه الدراسة أين تناولت من خلاله الطبيعة القانونية للجريمة المعلوماتية وأبرزت فيه خصائصها وخصائص مرتكبيها وأوجه الحماية الجزائية للنظم المعلوماتية في مواجهتها، كما تعرضت أيضا لموقف المشرع الجزائري منهذا النمط الإجرامي.

وما دفعني إلى تناول هذه المسائل هو المجرى المنطقي للأمور إذ لا يستقيم منطقا ولا عقلا أن يقوم المحققون من رجال الضبطية القضائية أو القضاء بالبحث عن الدليل لإثبات الجريمة المعلوماتية دون أن يكون لهؤلاء فهما موضوعيا لهذه الجريمة، ثم كرست الفصل الثاني للجوانب الإجرائية المتعلقة بمسألة التحقيق في الجريمة المعلوماتية، وفيها بينت الخصائص التي يتسم بها التحقيق وكذا الصفات التي يجب أن يتميز بها المحقق في هذا النمط الإجرامي، ثم فصّلت القول فذكرت خصائص الدليل الرقمي كدليل مناسب في إثبات الجريمة المعلوماتية، وأردفت ترتيبا على ذلك بتفصيل القواعد الإجرائية للحصول على الدليل الرقمي وانتهيت إلى تحديد القيمة القانونيةلهذا الدليل في مجال إثبات الجريمة المعلوماتية. وعلى أساس ذلك تحددت الإشكالية الجوهرية للبحث من خلال تحليل مدى تأثير التقنية المعلوماتية على الجانب الإجرائي للقانون الجزائي.

وعلىضوء الإشكاليات التي أظهرتها الدراسة خلصت في الإجابة عنها إلىجملة من النتائج كما يلي:

- إن مفهوم الجرائم المعلوماتية ينصرف إلى الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات، والتي تستهدف بشكل خاص المعلومات المختلفة في البيئة الرقمية، بالإضافة إلى كل جريمة ترتكب أويسهل ارتكابها بواسطة منظومة معلوماتية، وهذه الأخيرة في الغالب ما تكونجرائم تقليدية .
- إنمن أهم مميزات جرائم الاعتداء على نظم المعالجة الآلية للمعطيات،أنها تنصب على محل من نوع خاص يختلف تماما على محل الجرائم التقليدية فهذه الجرائم تستهدف المساس بالمعلومات

الإلكترونية المتواجدة في البيئة الرقمية على هيئة إشارات ونبضات غير مرئية تنساب عبر أجزاء النظام المعلوماتي وشبكات الإتصال العالمية.

- وقد تبين لي أنه ونظرا لكون النصوص الجزائية العقابية إنما وضعت للتعامل مع جرائم تنصب على محل مادي ملموس، فإن الأمر قد استتبعه قصور أوعجز هذه النصوص القانونية عن توفير الحماية الجزائية لمثل محل الجرائم المعلوماتية فكان ذلك من دواعي تدخل المشرع إلى إصدار نصوص جزائية تجرم بحق الأفعال التي تشكل اعتداء على نظم المعالجة الآلية للمعطيات وهو ما يقتضيه مبدأ الشرعية الموضوعية القائم على التفسير الضيق للنصوص القانونية العقابية وعدم جواز القياس.

- وقد توصلت أيضا إلى أن هذا القصور لم يعتر النصوص الموضوعية فقط و لم يقف عند الشق الموضوعي للقانون الجزائي، بل امتد تأثير التقنية المعلوماتية إلى الشق الإجرائي للقانون الجزائي، فقد أثارت هذه التقنية الحديثة العديد من الإشكالات في نطاقه ذلك أن نصوص قانون الإجراءات الجزئية إنما وضعت لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجزائي في الاقتناع.

- لذلك فقد توصلت في هذا البحث إلى أن الطبيعة الخاصة للجريمة المعلوماتية دعت المشرع إلى إعادة تقييمبعض القواعد الإجرائية المتاحة في استخلاص الدليل كالتفتيش والضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية، وهو ما كان فعلا بموجب القانون 09/04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، فضلا عن استحداث نوع من القواعد الإجرائية الأخرى تتلاءم مع الطبيعة الرقمية التي يكون عليها الدليل المناسب في إثباتهذا النوع من الجرائم كإعتراض المراسلات والمراقبة الإلكترونية.

وقد تبين معنا كذلك أن الدليل المناسب والأوفر في إثبات الجريمة المعلوماتية هو الدليل الرقمي والذي هو عبارة عن معلومات مخزنة في النظم المعلوماتية في شكل نبضات مغناطيسية أو كهربائية من الممكن من الناحية التقنية استخلاصه من البيئة الرقمية التي يتواجد بها، وتجميعه باستخدام برامج وتطبيقات تقنية، ليظهر بعد ذلك في شكل مخرجات إلكترونية أو حتى ورقية بعدطبعه.

كما أظهر البحث أيضا أن عملية استخلاص الدليل الرقمي سواء بالطرق الإجرائية التقليدية أوالمستحدثة ليس من السهولة بما كان، إذ تعوقها في غالب الأحيان صعوبات تتعلق إما بالطبيعة التكوينية للدليل الرقمي أو بالعامل البشري.

- إن الدليل الرقمي على ضوء ما أسفرت عليه التطورات التقنية في مجال المعلوماتية لا يغني عنه أن يكون مشروعا، وذلك بأن يتم الحصول عليه بالطرق القانونية وأن يقدم للمحكمة على نفس الهيئة التي تم جمعه عليها، بأن لا يطرأ عليه أي تغيير أو تحريف خلال فترة حفظه.
- إن الأدلة الرقمية وإن كانت تتمتع بقيمة علمية قاطعة في الدلالةعلى الحقائق التي تتضمنها، إلا أن الكشف عن الهوية الحقيقية للفاعل ليس بالأمر السهل فقد يمكن التعرف على هوية الحاسوب المستعمل في ارتكاب الجريمة والمرتبط بشبكة الإنترنت من خلال عنوان **IP** إلا أنه من الصعب تحديد هوية الفاعل ما لم يتم تدعيم هذا الدليل الرقمي بالأدلة التقليدية الأخرى فيما بعد.
- وقد لاحظت من خلال البحث حول مسألة تقدير القيمة القانونية للدليل الرقمي أنه يجب التمييز بين أمرين الأول : القيمة العلمية القاطعة للدليل الرقمي والثاني : الظروف والملابسات التي تحيط بهذا الدليل، فالقاضي ليس له أن ينازع فيما أسفرت عليه تكنولوجيا المعلوماتيةوالعلوم التقنية من الناحية العلمية وإنما له أن يقدر الظروف والملابسات التي أحاطت بهذا الدليل، ويمكن له في سبيل ذلك الإستعانة بطرق الإثبات التقليدية التي توجد عادة إلىجانب الدليل الرقمي، وله في ذلك أن يرفض هذا الدليل إذا لم يقتنع بظروف القضية وملابساتها.
- وهذا ما قادني إلى الوصول إلى نتيجة أخرى مؤداها تمتع القاضي الجزائي بدور إيجابي من حيث تقدير القيمة القانونية للدليل الرقمي وخضوعه للسلطة التقديرية، شأنه في ذلك شأن باقي الأدلة.
- كما تبين أن الإتصالاتالإلكترونية والنظم المعلوماتية تعتبر أحد أوجه الحياة الخاصة للإنسان ومظهرا من مظاهر خصوصياته ، وبالتالي فإن إجراءات استخلاص الدليل في البيئة الرقمية قد تؤدي إلى المساس بهذه الخصوصية وإمكانية إطلاع المحققين على أسرار خاصة بأشخاص قد لا يكون لهم أصلا يدٌ في الجريمة، مما جعل المشرع يحرص كل الحرص على هذه المسألة بأن اشترط

اللجوء إلى هذه الإجراءات إذا دعت إلى ذلك ضرورة التحري والتحقيق والتي يجب أن تقدر بقدرها.

- وفي الأخير فإنه وعلى هدي ما توصلت إليه في هذا البحث فإنه قد بدا لي أن أقدم جملة من المقترحات آمل أن أكون موفقا في طرحها.

- إن الجزائر وهي تخطوا الخطوات الأولى في تطبيق مشروع الحكومة الإلكترونية والذي من خلاله يتم السعي إلى استخدام تقنية المعلومات والاتصالات الإلكترونية في توفير وتقديم معلومات وخدمات الحكومة للمواطنين وجعلها متاحة للجمهور، فهذا المشروع لابد أن يستتبعه خطوة تشريعية هامةيكون الهدف منها توفير الحماية القانونية الشاملة لهذا المفهوم بصورة منسجمة ومتزامنة مع هذا التحول من أجل تخطي الثغرات القانونية التي قد يستفيد منها العابثون بأمن المعلومات، سيما وأن الأمر يتعلق بأنظمة معلوماتية تخص إدارات الدولة.

- حسب مفهوم المادة 44 من قانون الإجراءات الجزائية الفقرة الثانية المدرجة بموجب القانون 06/22 المؤرخ في 2006/12/20 فإنه لا يجوز لضباط الشرطة القضائية في إطار التحري والتحقيق عن الجرائم الماسة بأنظمة المعالجة للمعطيات الإنتقال إلى مساكن الأشخاص الذين يظهرون أنهم ساهموا في ارتكاب هذه الجريمة لإجراء التفتيش هناك إلا بإذن مكتوب من الجهة المختصة، مع وجوب استظهار هذا الإذن قبل الدخول إلى المسكن والشروع في عملية التفتيش،وعليه فالإذن في هذه المادة يتعلق حصرا بتفتيش المساكن ، لكن المشرع في القانون09/04 أجاز في إطار التحري والتحقيق في الجريمة المعلوماتية تفتيش محل آخر غير السكن وهو المنظومة المعلوماتية دون أن يشترط للدخول إليها ضرورة الحصول على إذن من الجهة القضائية المختصة، فحصول ضابط الشرطة القضائية على إذن يسمح له بالدخول إلى الأماكن التي تتواجد بها الحواسيب لا ينصرف في رأيي إلى الإذن بدخول المنظومة المعلوماتية لهذه الحواسيب وتفتيشها لاختلاف محل التفتيش أصلا ، لذلك أقترح على المشرع إضافة فقرة أخرى للمادة 05 من القانون 04/09 كما يلي "لا يجوز إجراء عمليات التفتيش في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة".

- سبق وأن مر بنا أن من بين الصعوبات في تحديد هوية المجرم المعلوماتي هو استعمال هذا الأخير لحواسيب غير شخصية في تنفيذ جريمته وغالبا ما تكون في مقاهي الإنترنت، هذه الأخيرة

التي يرتادها عدد كبير من الزبائن لا يمكن معرفة هواياهم ، لذلك أقترح على المشرع إعادة النظر في تسير هذه المقاهي وعدم اعتبارها مجرد نشاط تجاري كغيره من الأنشطة التجارية الأخرى، بل لابد من فرض أعباء والتزامات على مقدمي هذه الخدمة ومسيري مقاهي الإنترنت، كأن يطلب من أي زبون قبل شروعه في استعمالالإنترنتملء استمارة تحدد فيها كامل هويته والتوقيت الذي استعمل فيه شبكة الإنترنت ورقم جهاز الحاسوب الذي استعمله،كما يلتزم مسير المقهىبالاحتفاظ بعناوينالمواقع التي تم زيارها في ذاكرة كل حاسوب لمدة معينة، ونفس الشيء بالنسبة لاستعمال شبكات الإنترنت الموجودة في المؤسسات العامة كالجامعات وغيرها.

● ليس بالخفي أن هناك من الشركات الخاصة التي تحوي منظوماها المعلوماتية على المعلومات الشخصية أو الاسمية للعديد من المتعاملين معها، فالشركات المتخصصة في مجال الإتصالات مثلا،كمتعاملي الهاتف النقالتعتبر من خلال عدد المشتركين لديها بمثابة بنك للمعلومات الإسمية والتي يمكن التلاعب واستعمالها في أغراض غير مشروعة، لذلك اقترح على المشرع أن يتدخل لوضع القواعد القانونية الخاصة بالضمانات الوقائية للحياة الشخصية في إطار قانون متكامل يكون بمثابة مبادئ يقوم عليها نشاط نظم المعلومات الشخصية أو الإسمية وهذا الموضوع أرى أنه جدير بالبحث والمناقشة في دراسات لاحقة إن وفقني الله.

أرجوا أن أكون قد وقفت في معالجة هذا الموضوع، وإن لم أوفق فعذري أنني اجتهدت ولكل مجتهد نصيب.

قائمة المراجع

قـــائمة المراجع:

أولا: المصـــــــادر

1/القـــوانين

- الدستور الجزائري سنة 1996.
- قانون العقوبات المعدل والمتمم
- قانون الإجراءات الجزائية المعدل والمتمم
- قانون 04/09 المؤرخ في 14 شعبان 1430 الموافق لـــ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- قانون 03/2000 المؤرخ في 5 جمادى الأولى 1421 الموافق لـــ 5 أوت 2000 محدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

مرسوم رئاسي 183/04مؤرخ في 8 جمادى الأولى1425 الموافق لـــ 26 يونيو 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد القانوني الأساسي.

ثانيا: الكتب بـــاللغة العـــربية:

1/ الكتب العامـــة:

1. أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، دار هومة، طبعة 2003.
2. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية،دار النهضة العربية، 1996.
3. أشرف عبد القادر قنديل،النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي، دار الجامعة الجديدة ، طبعة 2011.
4. حاتم حسن موسى بكار، سلطة القاضي الجنائي في تقدير العقوبة والتدابير الإحترازية، الدار الجماهيرية للنشر والتوزيع والإعلان، الطبعة الأولى 2005.
5. فايز الإيعالي، قواعد الإجراءات الجزائية أو أصول المحاكمات الجزائيةعلى ضوء القانون والفقه والإجتهاد ، المؤسسة الحديثة للكتاب، الطبعة الأولى ،1994.
6. عبد الله سليمان ، شرح قانون العقوبات الجزائري القسم العام الجزء الأول (الجريمة)، ديوان المطبوعات الجامعية.

7. علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، المؤسسة الحديثة للكتاب،2006.

8. عبد الله أوهيبية، شرح قانون الإجراءات الجزائية الجزائري التحري والتحقيق، دار هومة، الطبعة 2003.

9. محمد محدة، ضمانات المتهم أثناء التحقيق،دار الهدى، الطبعة الأولى 1991-1992.

10. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الطبعة الثاثية2010.

11. محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة القاهرة، طبعة 2008.

2/الكتبالمـــتخصصة

1. أمير فرج يوسف:

- الجرائم المعلوماتية على شبكة الإنترنت، دار المطبوعات الجامعية الإسكندرية2009.
- الجريمة الإلكترونية والمعلوماتية، والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر الإنترنت، مكتبة الوفاء القانونية الإسكندرية، الطبعة الأولى 2011.

2. أحمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي الإسكندرية ، الطبعة الثانية، 2006.

3. إيهاب فوزي السقا، جريمة التزوير في المحررات الإلكترونية، دار الجامعة الجديدة للنشرالإسكندرية 2008.

4. الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية بحث فقهي مقارن، دار الفكر الجامعي ، الطبعة الأولى2011.

5. بولين أنطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية دراسة مقارنة ، منشورات الحلبي الحقوقية ، الطبعة الأولى 2009 .

6. خالد عياد الحلبي،إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع ، الطبعة الأولى 2011

7. خالد ممدوح إبراهيم:

- الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية ، الطبعة الأولى 2009.
- أمن الجريمةالالكترونية، الدار الجامعية، الإسكندرية، الطبعة 2008.

- فن التحقيق الجنائي في الجرائمالإلكترونية ،دار الفكر الجامعي الإسكندرية ، الطبعة الأولى 2009.

8. خثيرمسعود ، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى عين مليلة ، الطبعة 2010.

9. رشيدة بوكر ، جرائم الإعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن،منشورات الحلبي الحقوقية ، الطبعة الأولى2012.

10. شيماء عبد الغني محمد عطاالله ، الحماية الجنائية للتعاملات الإلكترونية ، دار الجامعة الجديدة ،2007.

11. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون،دراسة مقارنة ، منشورات الحلبي، الطبعة الثانية ،2007.

12.عادل عزام سقف الحيط،جرائم الذم و القدحو التحقير المرتكبة عبر الوسائط الالكترونيةدراسة قانونية مقارنة، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2011.

13.علي عدنان الفيل ، الإجرام الإلكترونيدراسة مقارنة، منشورات زين الحقوقية ، الطبعة الأولى2011.

14. عبد الفتاح بيومي حجازي :

- نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، منشأة المعارف ، الطبعة الأولى 2009.

-مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي الإسكندرية، الطبعة الأولى 2006.

- الإثبات الجنائي في جرائم الكمبيوتر والإنترنت ، دار الكتب القانونية ، 2007.

- الجريمة في عصر العولمة (دراسة في الظاهرة الإجرامية المعلوماتية) ، دار الفكر الجامعي، الطبعة الأولى 2007.

15. علي حسن محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب والإنترنت، عالم الكتب الحديثة، الطبعة الأولى 2004.

16. محمد طارق عبد الرؤوف الحن، جريمة الإحتيال عبر الإنترنت (الأحكام الموضوعية والأحكام الإجرائية) منشورات الحلبي الحقوقية ، الطبعة الأولى 2011

17. محمد أمين الشوابكة ، جرائم الحاسوب والإنترنت ""الجريمة المعلوماتية ""، دار الثقافة للنشر والتوزيع ، الطبعة الأولى 2009.

18. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن،دار الجامعة الجديدة الإسكندرية ،2007.

19. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة القاهرة، الطبعة الأولى 2009

20. محمد عبد الله أبو بكر سلامة ،جرائم الكمبيوتر والإنترنت ، منشأة المعارف،2006

21. محمود أحمد عبانة ، جرائم الحاسوب وأبعادها الدولية ، دار الثقافة للنشر والتوزيع ، الطبعة الأولى 2009.

22. منير محمد الجنبيهيوممدوح محمد الجنبيهي:

- جرائم الإنترنت والحاسب الآلي ووسائل مكافحتهما ، دار الفكر الجامعي 2004.
- أمن المعلومات الإلكترونية ، دار الفكر الجامعي 2006

23. نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي، الطبعة الأولى2005.

24.نهلة عبد القادر المومني، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع، الطبعة الثانية 2010.

25. هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، مكتبة الآلات الحديثة، الطبعة الأولى 1994

26. وضاح محمود الحمود ونشأت مفضي المجالي، جرائم الإنترنت،دار المنار للنشر والتوزيع 2005.

27. يونس عرب، قانون الكمبيوتر موسوعة القانون وتقنية المعلومات، منشورات إتحاد المصارف العربية، الطبعة الأولى2001.

ثالثا: الرسائل العلمية:

1. أبو المعالي محمد عيسى، الحاجة إلى تحديث آليات التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، ورقة مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون.

قــائمة المراجع:

2. صالح أحمد البربري ، دور الشرطة في مكافحة جرائم الإنترنت في إطار الإتفاقية الأوروبيةالموقعة في بودابست في 2001/11/23. بحث منشور على موقع www.arablawinfo.com.

3. طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية المنعقد في 28-29 /2009/10 لأكاديمية الدراسات العليا طرابلس.

4. عادل يوسف عبد النبي الشكري ، الجريمة المعلوماتية وأزمة الشرعية الجزائية، جامعة الكوفة، كلية القانون.

5. عبد الجبار الحنيص، الإستخدام غير المشروع لنظام الحاسوب في وجهة نظر القانون الجنائي، مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، المجلد 27، العدد الأول: 2001.

6. عبد الله حسين علي محمود ، إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات.

7. عمر محمد بن يونس ، الدليل الرقمي، بحث منشور على موقع www.arablawinfo.com.

8. عطا الله فشار،مواجهة الجريمة المعلوماتية في التشريع الجزائري، جامعة الجلفة.

9. محمد عيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحتين القانونية والفنية دراسة تطبيقية مقارنة ،جامعة نايف العربية للعلوم الأمنية، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي.

10.محمد أبو العلاء عقيدة ، التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية.

11.مفتاح بوبكر المطردي، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23-25 /2012/9 .

12. ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول TCP/IP في بحث وتحقيق الجرائم على الكمبيوتر، بحث منشور على موقع www.arablawinfo.com

13. موسى مسعود أرحومة ، الإشكالياتالإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، المؤتمر المغاربي الأول حول المعلوماتية والقانون خلال الفترة 28-29 /2009/10.

14.محروس نصار الغايب، الجريمة المعلوماتية، بحث مقدم من المعهد التقني جامعة الأنبار العراق.

رابعا: المراجع باللغة الأجنبية:

1/القـــوانين الفرنســـية:

1. Code pénal, Dalloz, paris 2009
2. Code de procédure pénal ,Dalloz, paris 2009
3. Loi n° 78/17 du 6 janvier relative à l'informatique aux fichiers et aux libertés.

2/ الكتب باللغة الفرنسية

1. Myriam QUEMENER :yves CHARPENEL .cybercriminalité Droit pénal appliqué .Normandie Roto impression 2010.
2. Christiane Féral –Schuhl .cybercriminalité le droit à l'épreuve de l'internet 6^em^édition –dalloz 2011.2012

3/ الرسائل العلمية باللغة الفرنسية

1. Offices fédérale de la polices. la cybercriminalité la face cachée de la révolution de l'information .rapport d'analyse stratégique : octobre 2001.
2. Département fédérale de justice et police .cybercriminalité Rapport de la commission d'experts .Berne juin 2003.
3. combattre cybercriminalité dans le respect des droits et libertés www.quadratre .net

فهرس المحتويات

فهـــرسة الموضـــوعات

ملــــــــــخص

يتلاءم موضوع هذه الدراسة مع التطورات الحديثة الحاصلة في مجال المعلوماتية التي أصبحت تشكل أداة لارتكاب الجريمة أو مجالا لها، وذلك بإساءة استخدامها و استغلالها على نحو غير مشروع. وقد سعيت من خلالها (هذه الدراسة) إلى توضيح القواعد الإجرائية التي على مداها يمارس العاملون في مجال البحث و التحري عن الجريمة المعلوماتية عملهم من أجل الحصول على الدليل المناسب لإثبات هذه الجرائم، وقد تناولت في الفصل الأول الجانب النظري للجريمة المعلوماتية من خلال مناقشة الجوانب القانونية لهذه الجريمة، وضمن هذا العنوان تم البحث في ماهية الجريمة المعلوماتية من خلال تحديد مفهوم المعلوماتية كشرط مفترض لقيامها، والتي تبين أنها تقوم أساسا على العلاقة بين المعلومات و التقنية الحديثة التي تستخدم في معالجة هذه المعلومات، لذلك كان من اللازم تعريف المعلومات و توضيح خصائصها وشروطها، ثم تناولت أيضا أهم التعريفات التي صاغها الفقه الجنائي للجريمة المعلوماتية وكذا الطبيعة القانونية الخاصة التي تميز هذه الجريمة عن غيرها من الجرائم التقليدية، وكذا الخصائص التي يتميز بها المجرم المعلوماتي وأهم الطوائف و الأصناف التي تنتمي إليها هذه الفئة من المجرمين، وماهي الأساليب و التقنيات المستعمله في ارتكاب الجريمة المعلوماتية، وكذا الدواوفع المحركة للمجرم المعلوماتي لارتكاب هذه الجريمة. ثم بعد ذلك تناولت مظاهر مكافحة الجريمة المعلوماتية على المستوى التشريعي سواء الوطني أم المقارنن وكذا الجهود المبذولة على المستوى الدولي في مكافحة هذه الجريمة، وفي الأخير تم طرح مسألة الإختصاص القضائي كأهم مشكلة تثيرها الجريمة المعلوماتية لكون النشاط الإجرامي فيها لا يعترف بالحدود.

وفي الفصل الثاني تم معالجة موضوع إجراءات تحصيل الدليل الرقمي لإثبات الجريمة المعلوماتية وأهم الجوانب القانونية لعملية التحقيق في هذه الجريمة، وهنا تناولت الأجهزة المؤهلة للبحث و التحري عن الجريمة المعلوماتية سواء في النظام القانوني الجزائري أو الأنظمة القانونية المقارنة، كما تم بعد ذلك البحث في الخصائص التي يتميز بها التحقيق و المحقق في الجريمة المعلوماتية، ثم تم تحديد مفهوم الدليل الرقمي من خلال توضيح خصائصه و أنواعه ومصادر الحصول عليه، وبعد ذلك تم التركيز بنوع من الشرح على القواعد الإجرائية المناسبة في عملية استخلاص الدليل الرقمي من بيئته الإلكترونية وتبيان أهم الصعوبات و المعوقات التي تواجهها هذه العملية .

كما تناولت في هذا الفصل أيضا ضمانات المشتبه فيه و أثر إجراءات الحصول على الدليل الرقمي على الحق في الخصوصية و أخيرا تناولت مسألة القيمة القانونية للدليل الرقمي في مجال الإثبات الجنائي سواء من حيث مشروعيته أم من حيث حجيته أمام القاضي الجزائي.

و في الخاتمة تم تبيان أهم النتائج التي تم التوصل إليها و وضع بعض التوصيات و الإقتراحات التي من شأنها تفعيل وتنظيم الإجراءات المناسبة للتحقيق في الجرائم المعلوماتية.

و الله ولي التوفيق.

Summary :

The subject of this study fits with the current modern happened in informatics scopewhich became a tool or a way for the perpetration of the crime byusing it in illegal purposes, through this study, I worked hard to clarify procedural rules, that are proceeded by the workers in searching and investigation field on informatics crimes, to obtain the right proof to prove these crimes, I have taken in the first chapter the theory hand of the informatics crime toward the discussion of the legal hands of this crime, within this title, we have searched for informatics crimes definitions through determining the concept of informatics as a supposed condition to complete it (proceed it), we revealed that it depends basically on the relation between informatics and modern technic used in treating these informations, this is why it was necessary to define informations and clarify its specifics and conditions, after that we mentioned the most important definition that was established by criminal philology for criminal informatics as well as the legal and special nature that specialize this crime from other traditional crimes and also the features of informatics criminal and the major sects and types that this kind of criminals belong to, and what are the used ways and technics in acting informatic crimes ,in addition to reasons of the informatic criminal behavior , after that I mentioned the legislative measures that had been taken to fight informatics crimes either on national or comparative level as well as the efforts that had been made on international in fighting this crime .

And finally we introduced the judicatory specialization as a main problem that causes informatics crime taking in consideration that criminal activity doesn't recognize limits.

In chapter two we dealt with the procedures of obtaining digital proof to prove informatics crime, and the most important and valid parts to complete the investigation in this crime, and there we treated the qualified instruments for researching and investigating informatics crimes , in Algerian laws likewise other legal comparative regimes, after that we searched through characteristics that specialize the investigation and investigator in informatic crime then we extracted the definition of digital proof through clarifying its characteristics and types and sources of obtaining it.

After that we concentrated descriptively on the appropriate measurement rules in the operation extracting digital proof from its electronic environment and gaining the major abstractions and difficulties in this operation.

In this chapter I also mentioned the guaranties of the suspect and the affections during the measures of obtaining digital proof on the right of privacy. in the end I dealt with the legal value of digital proof in criminal approving field whether it legislative or its persuasion in front of the penal judge.

In conclusion I clarified the most important results that have been obtained and putting some recommendations and suggestions that could be effective and helps to regulate the appropriate measures in investing informatic crimes.

God is the source of strength.